MISSION POUR L'ECONOMIE NUMERIQUE

Synthèse du guide technique pour la sécurité de la dématérialisation des achats publics

Version du 20 avril 2005

Objet du présent guide

Ce guide a été élaboré dans le cadre du groupe de travail « dématérialisation de l'achat public » de la mission pour l'économie numérique. Il a vocation a être modifié et enrichi progressivement. Il constitue, dans le domaine de la sécurité, un premier outil d'aide à destination de l'ensemble des acteurs de l'achat public. Il précise et justifie les bonnes pratiques de sécurité pour assurer aux procédures dématérialisées un niveau de sécurité globalement du même ordre que celui requis pour les procédures manuelles. Ce guide s'inscrit comme une brique complémentaire du vade-mecum juridique publié par le Minéfi.

La sécurité, une exigence incontournable de la dématérialisation des marchés publics

L'utilisation de nouveaux outils pour la mise en œuvre de la dématérialisation doit se faire dans le respect des obligations juridiques du Code des marchés publics et de la déontologie des acheteurs qui concernent :

1. l'égalité de traitement des entreprises ;
2. la transparence de la procédure ;
3. la confidentialité des offres ;
4. l'intégrité des Documents de Consultation des Entreprises et des offres ;
5. l'opposabilité et la traçabilité des actions des acheteurs et des entreprises (pouvoir démontrer qu'une personne a bien fait, ou n'a pas fait, une certaine action, insérée dans une chaîne d'événements) ;
6. la disponibilité des systèmes informatiques (s'assurer que les entreprises ne soient pas empêchées de remettre leur offre en raison d'une panne inopportune).

L'absence de précaution dans l'utilisation de l'informatique peut conduire rapidement à ne pas respecter l'un des principes ci-dessus énoncés et mettre en péril les procédures de marché en cours. C'est la raison pour laquelle, les personnes publiques doivent s'assurer que les systèmes destinés à gérer la dématérialisation, qu'ils soient mis en œuvre par elles-mêmes ou par des prestataires, respectent bien les obligations énoncées.

La sécurité de la dématérialisation des achats peut-elle se concevoir dans le cadre d'une utilisation ordinaire de l'informatique ?

Prenons un incident informatique classique, tel qu'une contamination par un virus. Si les conséquences restent supportables dans le cadre d'une utilisation ordinaire de l'informatique, elles peuvent être beaucoup plus graves dans une procédure de marchés publics.

Les mesures générales de sécurité

Mesures concernant le local

1. Le **local** où se trouve le poste doit être **fermé à clé** afin d'éviter les malveillances internes, ou même les simples indiscrétions.

2. Le **risque d'accident** (incendie par exemple) qui entraînerait la destruction non seulement des matériels (dommage qu'il est assez facile de quantifier) mais aussi des données qui y sont enregistrées (dommage plus difficile à quantifier, mais qui peut être beaucoup plus important), doit être examiné et les précautions jugées nécessaires doivent être prises.

Mesures concernant l'organisation ou le personnel

3. Les dispositifs et mesures techniques doivent être mis en œuvre par des **personnes suffisamment compétentes**, qu'elles appartiennent à l'entité (entreprise, personne publique) ou, si elle n'en dispose pas, qu'elles proviennent d'une assistance extérieure .

4. Les utilisateurs doivent pouvoir recourir à une **assistance technique** dans leurs opérations.

5. **Les documents doivent être vérifiés avant envoi** pour s'assurer qu'il s'agit bien de la dernière version et qu'elle ne contient plus de marques de révision ni d'informations non désirées.

6. Les utilisateurs doivent **être sensibilisés aux risques** que présente l'utilisation de leur ordinateur et d'internet. Ils doivent appliquer des règles de comportement prudent.

7. Des mesures techniques et organisationnelles doivent être prises pour préserver la **confidentialité des données sensibles** (outre bien sûr les candidatures et les offres, on peut citer le nom des entreprises candidates, des entreprises retenues, des entreprises qui ont remis une offre), vis à vis des **informaticiens** qui administrent le serveur et qui peuvent avoir besoin, de par leurs fonctions, d'accéder à ces fichiers. En particulier, ils ne doivent pas lire les candidatures et les offres des entreprises. Ces mesures reposent sur la définition précise de circonstances dans lesquelles les informaticiens devraient avoir accès à ces fichiers (par exemple en cas d'incident), l'attribution claire des rôles et des droits d'accès à ces données, et des mécanismes de contrôle d'accès.

Mesures concernant les postes de travail

8. **L'accès au poste de travail doit être protégé** au minimum par un mot de passe.

9. Les postes de travail doivent impérativement être équipés d'un **antivirus** tenu à jour quotidiennement. Pour une meilleure efficacité, cet antivirus ne doit pas être le même produit que celui du pare-feu .

10. Les postes de travail doivent également être équipés d'un produit de détection et d'éradication des espiogiciels (appelés aussi « **spyware** » : ce sont des programmes qui renvoient furtivement à l'extérieur des informations qui ne devraient pas sortir du poste). Ces programmes doivent être aussi tenus à jour. Ils doivent être mis en œuvre après chaque connexion par internet à des sites dont la confiance n'est pas établie.

11. **Les logiciels doivent être paramétrés** pour obtenir un bon niveau de sécurité (options par défaut examinées pour juger de leur intérêt et de leur dangerosité, options dangereuses désactivées).

12. Les vulnérabilités publiées sur les logiciels doivent être corrigées, en appliquant dès leur publication les **correctifs** proposés par l'éditeur.

13. Les **fichiers** importants, et notamment ceux qui doivent être conservés dans le cadre de la procédure, doivent être **sauvegardés** afin de ne pas les perdre en cas d'incident matériel ou logiciel sur les ordinateurs.

14. Il est recommandé de **chiffrer les fichiers sensibles**, en particulier s'ils sont stockés sur un serveur de fichiers.

15. Les postes raccordés à un réseau doivent être équipés d'un **pare-feu individuel** filtrant les accès entrants et sortants. Ce pare-feu doit être activé.

Mesures concernant le réseau

16. Le **raccordement à internet doit être filtré par un pare-feu**, équipé d'un antivirus tenu à jour en permanence.

Les mesures particulières de sécurité pour la personne responsable du marché (PRM) ou les acheteurs

1. **Les personnes intervenant dans les procédures de marchés doivent être sensibilisées aux risques** que présente l'informatique et connaître les mesures générales de sécurité (les mesures ci-dessus). Elles doivent également être formées à l'utilisation des outils informatiques particuliers à mettre en œuvre dans le cadre de la dématérialisation de l'achat ainsi qu'à la sécurité de ces outils. Elles devront connaître notamment la conduite à tenir en cas d'incident.

2. **Ces personnes doivent être identifiées** et leur rôle précisé ainsi que les droits qui s'y attachent (chargement, modification des fichiers sur la plate-forme, correspondance avec les entreprises, accès aux candidatures et aux offres, tenue du journal des événements…).

3. Un **contrôle des accès** doit être mis en place pour éviter que des personnes non habilitées interviennent à tort. Les personnes concernées doivent recevoir des moyens d'authentification (au moins des mots de passe) qu'elles ne doivent pas divulguer ni stocker sur leur poste de travail.

4. Le **règlement de la consultation** doit indiquer les formats[1] de fichier que la personne publique acceptera, les modalités selon lesquelles les entreprises devront transmettre leurs candidatures et leurs offres et notamment la façon de les chiffrer. Il indiquera également les modalités d'échanges avec les entreprises. Lorsque ces échanges devront se faire par messagerie électronique, il est nécessaire de deander aux destinataires de confirmer explicitement qu'ils ont reçu le message. L'utilisation de courriers électroniques recommandés (payants) permet d'obtenir automatiquement ces accusés de réception.

5. L'ouverture des candidatures et des offres doit s'accompagner des précautions nécessaires pour que celles-ci ne soient pas contaminées par les ordinateurs de la personne publique au cours de cette opération. Il conviendra d'attester s'il a été possible de réparer et de ne pas rejeter des documents porteurs de virus et la validité des documents ainsi acceptés. Il sera nécessaire de pouvoir justifier que les candidatures et les offres jugées irrecevables (celles reçues hors délai par exemple) n'ont pas été ouvertes. Il conviendra d'archiver tous les documents de façon opposable, avec les signatures qu'ils comportent et l'indication que ces signatures étaient valables quand elles ont été apposées. Un archivage de ces données sur cédérom devrait pouvoir être suffisant pendant quelques années.

Les mesures de sécurité concernant la plate-forme de dématérialisation

1. **La plate-forme**, qu'elle soit gérée par un prestataire ou par des agents de la personne publique **doit être sécurisée** (au minimum les mesures générales ci-dessus, d'autres mesures telles que la détection d'intrusions pouvant être recommandées).

2. Assurer un **contrôle anti-virus** des fichiers non chiffrés qu'elle reçoit, un contrôle antivirus quotidien des fichiers non chiffrés qu'elle détient et prévenir l'émetteur des fichiers porteurs de virus en tenant compte des dates de remises des plis.

3. Etre pourvue d'un **certificat de serveur**, pour s'authentifier auprès des entreprises qui la consultent. Ce certificat doit être publié d'une façon infalsifiable et commodément accessible, par exemple dans la presse. La plate-forme doit indiquer sur quel support il est possible de vérifier son certificat afin d'éviter que les entreprises ne soient amenées à s'adresser à un autre site se faisant passer pour la plate-forme.

4. Garantir **l'intégrité et l'origine des documents** qui lui sont confiés.

5. Fournir un **accusé de réception** des documents qui lui sont transmis.

6. Garantir la **confidentialité des informations** qui lui sont confiées. Elle ne doit recevoir les candidatures et les offres que chiffrées. Pour les informations non chiffrées (nom des entreprises candidates et des entreprises admises à concourir, nom des entreprises qui ont remis une offre, échanges avec les entreprises…) la confidentialité doit être garantie par des mesures techniques et orga-nisationnelles. C'est

[1] Autoriser chaque fois que c'est possible les formats qui peuvent être lus par des logiciels gratuits, privilégier les formats qui ne peuvent pas être modifiés accidentellement, comme le « portable document format » (.pdf)

possible en assurant notamment le contrôle des accès du personnel aux moyens in-formatiques et en prenant des engagements de confidentialité.

7. Fournir les **clés de chiffrement et de déchiffrement** (directement ou en s'adressant à un prestataire tiers de confiance). La clé de déchiffrement nécessaire pour procéder à l'ouverture des candidatures et des offres ne doit être connue que de la PRM. Il convient donc de s'assurer de sa qualité et de sa confidentialité.

8. Séquestrer ou faire séquestrer les clés de déchiffrement afin d'être en mesure d'en fournir une copie à la PRM en cas de nécessité (ce séquestre doit être fait de façon à ce que la confidentialité des clés soit absolument préservée).

9. Fournir un mécanisme qui permette de garantir que **les candidatures et les offres jugées irrecevables** n'ont pas été ouvertes.

10. Assurer la **confidentialité en transmission** de toutes informations qu'elle échange avec les entreprises et la personne publique par le web, par exemple en utilisant le protocole SSL.

11. Horodater et tracer de façon fiable et opposable toutes les actions où elle intervient, garantir que tous les fichiers qui lui ont été remis restent disponibles au moins jusqu'à la fin de la procédure, et donc en particulier être en mesure de démontrer qu'aucun n'a été perdu.

12. Mettre en place des **procédures de surveillance de la disponibilité** et d'alerte de la PRM et des acheteurs, au moins aux périodes de remise des candidatures et des offres. Mettre en place un dispositif d'information des internautes en cas d'indisponibilité de la plate-forme. Disposer de raccordements à internet de débit suffisant face au volume des fichiers qu'elle recevra et émettra.

13. Etre pourvue de systèmes de **contrôle d'accès**, aussi bien pour les opérations qu'y effectuent les entreprises et la PRM que pour les opérations techniques des informaticiens qui la mettent en œuvre ; ces accès doivent être journalisés.

14. La **politique de sécurité** doit être affichée sur le site internet. Les entreprises sauront avec quel soin les documents transmis seront traités. Les différentes versions doivent être datées et numérotées.

Les responsabilités de la maîtrise d'ouvrage des achats

Il est de sa responsabilité de choisir les prestataires de dématérialisation et d'organiser les processus spécifiques à la dématérialisation.

Si la personne publique acquiert un progiciel

1. S'assurer que le progiciel remplit bien les fonctions de sécurité indiquées ci-dessus pour la plate-forme et des garanties de **pérennité et de maintenabilité.**

2. S'assurer que le contrat prévoit la réversibilité nécessaire.

3. Déterminer **quelles responsabilités l'éditeur accepte de prendre** en cas de dysfonctionnement de son produit.

Si la personne publique recourt à un prestataire

Si un prestataire gère la plate-forme d'achats dématérialisés, certaines **précautions supplémentaires** sont à prendre pour assurer la sécurité de la prestation. Il convient de rappeler que la responsabilité de la personne publique reste engagée, même dans le cas d'une externalisation du service. Il est donc nécessaire de rédiger les clauses du contrat liant la personne publique à son prestataire de manière précise. Il faut clairement identifier le périmètre, la nature des prestations fournies et les engagements de chacune des parties. La vérification annuelle du respect de ces clauses garantit, dans ce contexte, la transparence du processus dématérialisé d'achat public pour chacune des parties mais aussi pour les entreprises soumissionnaires.

Les responsabilités des informaticiens de la personne publique

Les informaticiens de la personne publique sont responsables du choix et du fonctionnement des moyens informatiques internes. Ils doivent contribuer au choix des prestataires. Les obligations de sécurité de ceux qui administrent une plate-forme gérée en interne sont décrites ci-dessus. Ils doivent **également mettre en place les procédures et les outils nécessaires pour que la PRM et les acheteurs** puissent effectuer les opérations qui leur incombent dans de bonnes conditions de sécurité (sauvegardes, contrôle et journalisation des accès, contrôles anti-virus etc.).
s obligations des soumissionnaires (pour les réponses aux appels d'offres formalisés)

1. **Acquérir un certificat** d'un prestataire de services de certification référencé par la plate-forme, à l'usage exclusif de la personne qui signera la candidature et l'offre (ce certificat de signature ne sera pas utilisé pour le chiffrement).

2. **Après avoir signé la candidature et l'offre, il convient de les chiffrer** par les moyens que la personne publique aura mis à disposition. Ils sont intégrés à la plate-forme de dématérialisation.

3. Lorsque les **échanges** avec la personne publique doivent se faire par messagerie électronique, il faut **demander** aux destinataires de confirmer explicitement qu'ils ont reçu le message. L'utilisation de courriers électroniques recommandés (payants) permet d'obtenir automatiquement ces accusés de réception.

4. Prendre les précautions nécessaires pour que les **fichiers volumineux** qu'elle adresse à la personne publique lui parviennent dans les délais nécessaires, en tenant compte de l'autorisation éventuelle du double envoi (cf *vademecum juridique*, § 9.6).

Dernière recommandation

Il ne suffit pas d'édicter des règles générales de sécurité et de s'en remettre à la bonne volonté des intervenants pour les appliquer. Dans chaque entité, entreprise, personne publique ou prestataire, **une personne** doit être **chargée de la sécurité** des systèmes d'information. Son rôle est de préciser les consignes décrites ci-dessus, d'organiser la sensibilisation des intervenants, de veiller à l'application des consignes, de se faire rendre compte des incidents éventuels et d'en tirer les enseignements. L'objectif est d'être en mesure de **démontrer**, en cas de litige, **qu'il n'y pas eu de négligence**.