MISSION POUR L'ECONOMIE NUMERIQUE

GUIDE TECHNIQUE POUR LA SECURITE

DE LA DEMATERIALISATION DES ACHATS PUBLICS

Version du 20 avril 2005

Animateur du groupe de travail: J.F PACAULT

SOMMAIRE

Introduction

La dématérialisation des procédures de passation des marchés publics, introduite par le code des marchés publics (CMP) adopté en 2001, engage un processus de modernisation de la commande publique et d'amélioration de son efficacité. Pour les acheteurs publics, elle les incitera à rationaliser leur organisation d'achat et leurs procédures, d'où ils tireront une meilleure efficacité économique. Les entreprises, de leur côté, bénéficieront d'une publicité élargie des procédures engagées, accéderont plus facilement aux documents de ces consultations et pourront présenter leurs candidatures et leurs offres plus commodément et plus rapidement. Toutefois un minimum de précautions, techniques, d'organisation, de formation et sensibilisation des personnels, doivent être prises, par les personnes publiques aussi bien que par les entreprises, pour que la sécurité des procédures dématérialisées ne soit pas inférieure à celle des procédures existant auparavant.

En complément du vade-mecum juridique publié par le Ministère de l'économie, des finances et de l'industrie http://www.minefi.gouv.fr/daj/marches_publics/vademecum/vmdemat.htm, le présent guide est destiné à la fois aux entreprises qui choisissent les procédures dématérialisées et aux personnes publiques ; les entreprises pour qu'elles puissent conserver, dans les procédures dématérialisées, le niveau de sécurité des procédures actuelles ; les personnes publiques puisque ce sont elles qui endossent la responsabilité des dysfonctionnements éventuels et de leurs conséquences, qu'ils soient de leur fait, du fait des produits qu'elles ont mis en œuvre, du fait de leurs prestataires, ou du fait des produits et des procédures dont elles imposent l'usage aux entreprises. Les unes et les autres doivent donc prendre elles-mêmes un certain nombre de précautions ; les personnes publiques doivent de plus obtenir, de la part de leurs éventuels prestataires et fournisseurs, les engagements qu'ils appliquent bien les mesures de sécurité pour ce qui les concerne.

Ce guide a donc pour but de donner un éclairage technique sur les problèmes de sécurité que comporte la dématérialisation des marchés publics et de proposer, en les justifiant, les mesures de sécurité qu'il est judicieux de prendre pour assurer aux procédures dématérialisées un niveau de sécurité globalement du même ordre que celui requis pour les procédures manuelles.

La sécurité totale est inaccessible et l'ensemble des mesures ne prétend donc pas y atteindre ; ce guide est simplement un ensemble de bonnes pratiques pour ramener dans la plupart des cas les risques à un niveau jugé acceptable, c'est à dire globalement du même ordre que celui accepté pour les procédures manuelles. D'autres façons de faire peuvent sans doute apporter un niveau de sécurité comparable, et même supérieur : il appartient donc aux personnes publiques et aux entreprises, si elles envisagent d'autres façons de faire, d'apprécier le niveau de sécurité qu'elles leur apportent, et de s'assurer qu'il est bien adapté à leurs besoins.

Le public visé par ce guide est vaste, puisqu'il s'agit de toutes les personnes publiques, qui sont dorénavant obligées d'accepter les candidatures et offres dématérialisées et des entreprises qui souhaitent profiter de la dématérialisation ; les compétences techniques, parmi ce public, sont donc probablement très diverses et les moyens qui seront mis en œuvre aussi, fonction entre autres de ces compétences diverses. Toutefois on s'efforce d'abord d'aider ceux qui craignent de ne pas avoir suffisamment de compétences en propre, pour leur permettre d'organiser leur sécurité, de faire des choix éclairés et d'obtenir de leurs fournisseurs le niveau de sécurité nécessaire.

Ce guide comporte :

- des généralités sur la sécurité des systèmes d'information qui, comme les systèmes de dématérialisation des achats publics, viennent compléter, et parfois remplacer des procédures manuelles : il est nécessaire d'obtenir un niveau de sécurité globalement du même ordre que celui requis pour les procédures manuelles, ce qui nécessite en général, outre la mise en place de dispositifs techniques, une plus grande rigueur dans l'organisation et des compléments de formation des personnels;

- un exposé d'ensemble sur les besoins de sécurité des procédures d'achat dématérialisées;

- pour les entreprises, la plate-forme de dématérialisation, la PRM et les acheteurs, et enfin les informaticiens de la personne publique, une liste des mesures de sécurité spécifiques à la dématérialisation ;

- les mesures générales de sécurité à prendre pour tout système informatique, en particulier s'il est raccordé à internet.

1 Généralités sur la sécurité d'un nouveau système d'information : conserver le niveau de sécurité initial et s'adapter au niveau des attaques possibles

1.1 Classification des besoins de sécurité

- **confidentialité** : qualité d'une information ou d'un processus de n'être connue que par les personnes ayant besoin de la connaître ;

- **intégrité :** qualité d'une information ou d'un processus de ne pas être altérée, détruite ou perdue par accident ou malveillance ;

- **disponibilité :** qualité d'une information ou d'un processus d'être, à la demande, utilisable par une personne ou un système ;

- **opposabilité :** qualité d'une information ou d'un processus d'être produit comme preuve de la réalité d'une action (non-répudiabilité d'une action) ;

- **traçabilité :** qualité d'une information ou d'un processus d'être reconnu comme inséré dans une chaîne séquentielle d'événements.

Ces besoins ne sont donc pas particuliers aux systèmes informatisés, mais l'informatisation oblige à les formaliser plus soigneusement. Pour chaque système, ils doivent être grossièrement quantifiés en fort, moyen, faible en fonction de la gravité des conséquences qu'il y aurait à ne pas les satisfaire.

1.2 Obtenir un niveau de sécurité conforme aux obligations posées par les textes en vigueur et équivalent à celui requis pour les procédures manuelles

- les pannes et dysfonctionnements ne doivent pas être plus fréquents ;

- les attaques et malveillances ne doivent pas être plus faciles à réaliser ;

- leurs conséquences en cas de réalisation ne doivent pas être plus graves. Par exemple, il est possible d'intercepter un courrier postal et d'en prendre connaissance, mais c'est à chaque fois une opération qui comporte des risques pour l'attaquant, risques qui s'accumulent quand elle est répétée. Il est donc probable que de telles attaques resteraient ponctuelles. Il est peut être un peu plus difficile, du moins sans quelques compétences techniques, d'intercepter un courrier électronique ordinaire (non chiffré et non signé) pour en prendre connaissance voire le modifier, mais après un premier succès l'opération peut être répétée sans risque supplémentaire ;

- les risques qui n'existent que par l'utilisation de l'informatique (virus par exemple) doivent être traités.

Il faut noter que les procédures manuelles comportent, de fait, de nombreux contrôles et vérifications implicites et non formalisés. Ils attirent l'attention sur d'éventuelles anomalies et apportent donc une certaine protection. Il est certainement très difficile de formaliser et donc d'automatiser ces contrôles

et vérifications, qui par conséquent disparaissent avec l'informatisation. Inversement bien sûr, le risque d'erreurs humaines peut diminuer.

2 Mesures de sécurité des systèmes d'information

La sévérité des attaques dont il faut se protéger est très variable. Tout au plus peut-on penser que les précautions doivent être d'autant plus soignées que les enjeux du système à protéger sont plus importants. Pour les marchés dématérialisés, ont probablement une sensibilité particulière les marchés importants et ceux pour lesquels un incident aurait des conséquences particulièrement dommageables pour la personne publique.

2.1 Les mesures à prendre sont de plusieurs nature :

- **techniques :** mise en place de dispositifs informatiques de protection (antivirus, pare-feu etc.) ;
- **physiques :** accès contrôlés aux locaux sensibles, protection contre les accidents… ;
- **relatives à l'organisation du système :** procédures, consignes claires aux personnels, attribution des responsabilités ;
- **juridiques :** dispositions contractuelles spécifiques avec les prestataires et fournisseurs de progiciels ;
- **relatives aux personnels** : sensibilisation à la sécurité, formation aux procédures et à la mise en œuvre des outils informatiques, mais aussi engagements de confidentialité, en particulier de la part de prestataires extérieurs (cf. vade-mecum juridique § 9.4). Comme pour les procédures manuelles, il est aussi judicieux de veiller à ne pas affecter à certaines tâches des personnes qui présenteraient des conflits d'intérêt.

Il est évident que les outils techniques, aussi performants soient-ils, ne valent que par la façon dont ils sont mis en œuvre et l'environnement où on les exploite : les mesures techniques sont en général inopérantes, ou du moins très insuffisantes, si les autres mesures n'ont pas été prévues d'abord : les protections techniques ne viennent qu'à l'appui et en complément de ces autres mesures.

2.2 Objets des mesures de sécurité

- **dissuader** les éventuels attaquants. La première dissuasion est la menace de sanctions pénales (cf. code pénal, article 323 pour les délits informatiques) ou disciplinaires si le règlement intérieur les prévoit ou si une malveillance nécessite d'enfreindre un engagement écrit. D'autres mesures dissuasives sont de rendre difficile l'accès illégitime, ce qui détournera les attaques peu compétentes ou peu motivées, d'authentifier et de tracer efficacement les actions effectuées sur le système, en le faisant savoir : la probabilité de détecter les malveillances et de les imputer à leur auteur s'accroît et peut suffire à dissuader les malveillances etc.

- **protéger** au mieux les systèmes contre les attaques et les pannes : contrôles d'accès, gestion des droits, mécanismes de sécurité aussi forts que nécessaire, assurances de bon fonctionnement, *« back-up »* ;

- **détecter** les incidents et, pour les attaques éventuellement réalisées, tenter d'identifier leur origine ; ceci nécessite au moins que toutes les transactions effectuées soient enregistrées, pour pouvoir reconstituer les événements qui auraient conduit à un incident (ceci nécessite en général des outils d'analyse de fichiers volumineux, pour détecter les anomalies dans le flot des transactions effectuées) ; mettre en place éventuellement un système de détection des attaques en temps réel ;

- **réparer** les dommages éventuellement causés : avoir un système de « back-up » et des outils de restauration

En général, une même mesure contribue à plusieurs des grands principes énoncés ci-dessus. Par exemple un bon système de contrôle d'accès protège de ceux qui n'ont pas d'accès légitime en même temps

qu'il dissuade les malveillances internes, de la part de ceux qui ont un accès légitime : ils seraient en effet les premiers soupçonnés en cas d'attaque, puisque la probabilité d'attaque externe est réduite par l'efficacité du contrôle d'accès. Symétriquement, les mesures de sécurité doivent se renforcer mutuellement, pour qu'au cas où l'une d'elles serait défaillante (par suite de panne, d'erreur humaine, d'imperfections des logiciels etc.) la sécurité de l'ensemble ne soit pas totalement compromise.

Il est clair cependant qu'aucun ensemble de mesures de sécurité, aussi complet et performant soit-il à l'origine, ne peut suffire indéfiniment, sans même parler du relâchement dans leur application qui se produit souvent au fil du temps et qui doit bien sûr être combattu. On sait en effet que de nouveaux modes d'attaque apparaissent continuellement :

- par l'exploitation de vulnérabilités plus ou moins récemment découvertes dans les produits utilisés ;
- mais aussi par de nouvelles méthodes ou combinaison de méthodes, sans forcément qu'il y ait d'innovation technique.

Il est indispensable, pour le premier cas, de corriger régulièrement les vulnérabilités découvertes dans les produits, en appliquant les correctifs que publient les éditeurs de logiciels. Par contre, pour le second cas, il peut être nécessaire de modifier l'architecture des systèmes, en y rajoutant des dispositifs de protection, de modifier les consignes données aux personnels et de les sensibiliser particulièrement à ces nouvelles méthodes d'attaque[1].

3 Exigences de sécurité pour les marchés publics dématérialisés

Pour les marchés publics dématérialisés, la nécessité de la sécurité découle des obligations juridiques fixées par le code des marchés publics, ses décrets d'application relatifs à la dématérialisation qui disposent notamment que la personne publique " assure la sécurité des transactions sur un réseau informatique accessible à tous les candidats de façon non discriminatoire " et des dispositions légales et réglementaires relatives à la protection des données personnelles. Elle découle également de la déontologie qui doit être celle des acheteurs publics et des informaticiens.

Il existe une **différence importante entre une procédure dématérialisée d'achat public et une procédure de télédéclaration**, par exemple TéléTVA : un incident avéré sur TéléTVA se réglerait en bilatéral, entre le fisc et l'entreprise affectée, sans conséquence sur d'autres entreprises.

En revanche un incident sur une procédure d'achat dématérialisée peut avoir des conséquences sur toute la procédure en cours. Par conséquent, toutes les entreprises qui y participent peuvent être affectées, sans parler des complications et retards subis par l'acheteur. De tels incidents pourraient être, entre autres, la corruption des documents (AAPC, DCE…) émis par l'acheteur, corruption qui induirait en erreur les entreprises consultées, lesquelles seraient fondées à protester. Ce pourrait être aussi la divulgation de certaines offres reçues par la PRM dans des conditions qui permettraient à des concurrents d'en tirer parti ; on peut aussi citer des attaques sur un serveur, qui empêcheraient certaines entreprises de remettre leur offre dans les délais impartis, etc. De tels incidents sont couramment constatés sur internet et leurs conséquences sur une procédure d'achat dématérialisée seraient telles qu'il faut donc s'en protéger sérieusement.

[1] Par exemple, quand les virus transmis en pièce jointe à des courriers électroniques ont fait leur apparition, il y a quelques années, des consignes de vigilance ont dû être données aux utilisateurs, en même temps que des anti-virus étaient installés sur les serveurs de courrier. De même, l'apparition récente du « phishing », attaque par laquelle les internautes son dirigés vers de faux sites, la plupart imitant le site de leur banque, où ils sont amenés à divulguer leurs mots de passe, numéros de carte bancaire etc. nécessite à la fois que les sites susceptibles d'être ainsi imités soient certifiés (mesure technique, cf. annexe 2), que les clients apprennent à vérifier ces certificats, et qu'ils soient de toutes façon méfiants quand il leur est demandé de fournir des informations confidentielles sur internet (mesures de sensibilisation des personnes).

Précautions particulières pour l'utilisation d'un progiciel ou le recours à un prestataire :

Les enjeux d'une procédure d'achat public sont variables, mais les risques juridiques encourus par la personne publique restent les mêmes, quels que soient les enjeux de la consultation. Si la procédure n'est pas dématérialisée, on peut estimer que la personne publique dispose de tous les moyens de maîtriser ces risques ; il n'en est plus tout à fait de même quand la procédure est dématérialisée.

En effet, pour s'acquitter de son obligation d'accepter les candidatures et les offres dématérialisées, la personne publique utilisera le plus souvent des matériels et des logiciels, constituant une « plate-forme » de dématérialisation[2]. C'est par cette plate-forme qu'elle mettra à la disposition des entreprises les documents relatifs à la procédure (AAPC, dossier d'appel à candidatures, DCE) et que les entreprises lui soumettront leurs candidatures et leurs offres, le tout dans les conditions de sécurité nécessaires.

La personne publique peut choisir d'opérer elle-même cette plate-forme : elle devra donc acquérir les matériels et les logiciels nécessaires, et les mettra en œuvre elle-même. Il reste dans ce cas qu'elle ne maîtrise pas totalement le bon fonctionnement du logiciel de dématérialisation qu'elle met en œuvre. Avant de choisir ce logiciel, la personne publique doit donc s'assurer qu'il assure bien le niveau de sécurité nécessaire (cf. § « mesures de sécurité concernant l'entreprise » ci-après) et examiner quelle part de responsabilité l'éditeur du logiciel accepte de prendre en cas de dysfonctionnement.

Ou bien la personne publique peut recourir à un prestataire qui met en œuvre une plate-forme pour de multiples clients : cette solution a l'avantage de décharger la personne publique du soin d'administrer techniquement la plate-forme, et donc lui évite de disposer elle-même des compétences techniques nécessaires. Il est évident que dans ce cas la personne publique maîtrise encore moins les risques éventuels. Comme dans le cas ci-dessus de l'achat d'un logiciel, elle doit donc obtenir du prestataire des garanties quant au niveau de sécurité de la plate-forme et comment il assume sa part de responsabilité dans les éventuels dysfonctionnements. Il faut en particulier veiller à ce que le prestataire n'ait pas accès aux informations confidentielles de la procédure.

Enfin le recours à un prestataire établi à l'étranger, et en particulier hors de l'Union européenne, est à examiner avec soin, notamment du point de vue juridique ; en effet, les lois auxquelles il est soumis dans le pays où il est établi peuvent être sensiblement différentes des lois françaises, par exemple pour la protection des données personnelles[3] et pour l'utilisation du chiffrement qui est sévèrement réglementé dans certains pays[4]: il faut donc que la personne publique obtienne d'un tel prestataire toutes les informations qui lui permettent de s'assurer que les obligations de la législation française seront remplies en dépit des différences qui existent avec la législation du pays d'établissement du prestataire.

Les annexes 10 et 11 indiquent quelques précautions à prendre pour le recours à un prestataire et l'acquisition d'un progiciel.

[2] D'autres solutions techniques sont envisageables, comme par exemple l'utilisation de courriers électroniques recommandés (chiffrés, signés et horodatés en tant que de besoin, notamment pour les offres) : de telles solutions se calquent plus fidèlement sur les procédures non dématérialisées que connaissent bien les acheteurs ; même si elles peuvent être techniquement plus simples, d'une part elles ne dispensent pas de précautions de sécurité et d'autre part, étant moins automatisées, elles laissent entièrement à la charge des participants diverses opérations qu'une plate-forme soit réalise automatiquement (chiffrement, contrôles d'intégrité, sauvegarde de fichiers importants…) soit pour lesquelles elle apporte une assistance (journalisation d'évènements par exemple).

[3] Voir notamment http://www.cnil.fr/index.php ?id=1154

[4] ce qui pourrait avoir pour effet de rendre inopérantes les précautions prises pour assurer la confidentialité des candidatures et des offres (mécanismes de chiffrement obligatoirement faibles, accès aux clés de chiffrement par des tiers étrangers à la procédure…)

3.1 Identification des besoins de sécurité les plus évidents

- les documents émis par la personne publique doivent être intègres et souvent opposables ;
- les offres des entreprises doivent être intègres, confidentielles et opposables ;
- la liste des entreprises en compétition doit être confidentielle.
- Il faut que rien n'empêche, ni de la part de la personne publique ni de la part de ses prestataires éventuels, que les candidatures et offres soient remises dans les délais fixés, ce qui nécessite donc que le système de réception des offres ait une forte disponibilité ;
- Il est nécessaire que certaines actions réalisées par la personne publique comme par les entreprises soient tracées de façon fiable, et que l'heure à laquelle elles ont été effectuées soit connue, de façon fiable et avec une précision suffisante.

D'autres besoins existent également. Ils apparaissent au paragraphe « Mesures de sécurité par type d'acteur » ci-après, avec les mesures de sécurité correspondantes.

3.2 Quantification des besoins de sécurité

Les besoins de sécurité sont quantifiés comme suit en fonction des conséquences à redouter :

3 : la procédure peut être invalidée ou on risque une distorsion de la concurrence (divulgation de propositions d'une entreprise, empêchement de certaines entreprises de concourir par exemple),

2 : gêne significative pour le déroulement de la procédure, divulgation d'informations devant rester confidentielles au moins lors de leur divulgation (par exemple liste des fournisseurs admis à concourir),

1 : gêne supportable.

Pour la disponibilité en particulier, on considérera que si le besoin est de niveau 3, une indisponibilité supérieure à 2 heures n'est pas acceptable. S'il est de niveau 2, l'indisponibilité ne doit pas être supérieure à 12 heures, et à 24 heures pour le niveau 1. Ces durées sont en effet un compromis acceptable entre les besoins théoriques – on exigerait volontiers, par exemple, une disponibilité totale vers la fin de la période de remise des offres – et le coût qu'il y aurait à satisfaire ces besoins théoriques. Dans les 3 cas, l'indisponibilité doit faire l'objet d'une surveillance et d'alertes des utilisateurs.

On voit donc, sur ce point particulier de la disponibilité, qu'il subsiste des risques résiduels même si le besoin de sécurité affiché est satisfait. Il en est de même pour les autres besoins. Par conséquent il faut prévoir comment gérer ces risques résiduels, pour en atténuer les conséquences dommageables. L'annexe 7 propose quelques mesures pour atténuer les conséquences des **incidents d'origine technique**, c'est à dire qui sont propres aux procédures dématérialisées.

Comme le prescrivent le CMP et le vade-mecum juridique, les candidatures et les offres dématérialisées pour un marché formalisé doivent être signées électroniquement par la personne de l'entreprise qui en endosse la responsabilité. Cette signature est apposée en utilisant un certificat (cf.annexe 2) , qui, comme le précise le vade-mecum, doit répondre au moins aux exigences de la PRIS niveau 2. De plus il peut être utile que ces personnes utilisent ce certificat pour signer aussi d'autres documents, même si aucune obligation juridique ne l'impose, voire que d'autres personnes ou entités (serveur informatique par exemple) signent également des documents : c'est en effet un moyen de garantir l'intégrité et l'origine des documents, moyen dont la mise en œuvre est commode pour ceux qui en sont déjà dotés et pour leurs correspondants.

Il n'y a par contre aucune obligation juridique que les employés de la personne publique, les PRM par exemple, apposent des signatures électroniques sauf pour signer le marché lui-même (cf. vade-mecum juridique § 11, qui prescrit que la PRM utilise alors un certificat PRIS niveau 2). Pour les étapes de la procédure couvertes par le présent guide (c'est à dire de la publication de l'AAPC jusqu'au choix du fournisseur), il n'est donc pas nécessaire qu'elles soient dotées d'un certificat. L'intégrité et l'origine des documents qu'elles émettent doivent donc être assurées par d'autres moyens (vérifications manuelles avant la mise en ligne, contrôles d'accès à la plate-forme assurant que seules les personnes habilitées peuvent y enregistrer les documents, et bien sûr certification du serveur de la plate-forme).

3.3 Remarques sur la portée juridique de la signature de niveau 2 de la PRIS

Comme tout écrit, électronique ou non, une signature électronique peut être contestée en justice. Si cette signature répond aux conditions posées par le décret n° 2000-272 du 30 mars 2001, elle est présumée fiable et c'est à celui qui la conteste qu'il revient d'apporter au juge la preuve que cette signature n'est pas fiable. Dans les autres cas, c'est à celui qui la considère comme valable d'en convaincre le juge.

Or la signature de niveau 2 de la PRIS, niveau estimé suffisant en général pour la dématérialisation des marchés publics, ne répond pas aux conditions du décret n° 2000-272 du 30 mars 2001: la personne publique doit donc être en mesure, si le besoin apparaît, de convaincre un juge que les signatures utilisées dans le processus de dématérialisation sont valables. Ceci concerne aussi bien les signatures numériques qu'elle a apposées elle-même, que celles qu'ont apposées les entreprises, sur ses conseils et en prenant les précautions qu'elle indique.

Cette conviction ne pourra être emportée que si :

- les mesures d'organisation entourant la signature sont clairement explicitées, montrant que le risque d'un mauvais usage de la signature est négligeable ;

- il est possible de démontrer que ces mesures sont bien appliquées par la personne publique, qu'elles ont été clairement portées à la connaissance des entreprises pour ce qui les concerne, et qu'elles y sont applicables sans difficulté particulière ;

- les produits informatiques utilisés pour la signature sont raisonnablement fiables s'ils sont correctement utilisés, aussi bien ceux que la personne publique utilise elle-même que ceux qu'elle recommande (voire impose) aux entreprises.

Les mesures proposées ci-après intègrent cette préoccupation. En fonction des enjeux d'un marché, des difficultés qu'elle prévoirait à convaincre un juge de la fiabilité d'une signature numérique, ou de toute autre considération, la personne publique peut parfaitement exiger une signature conforme au niveau 3 de la PRIS, qui est réputée fiable. De même une entreprise peut estimer nécessaire de se doter de certificats de niveau 3, si la protection supplémentaire qu'ils apportent, et leur sécurité juridique lui paraissent indispensables.

3.4 Horodatage

Une exigence juridique fondamentale est qu'un certain nombre d'actions soient **datées** de façon fiable, comme celles qui marquent le départ d'un délai réglementaire (délai de remise des candidatures) ou celles qui doivent être accomplies avant une date limite (remise des candidatures, remise des offres).

Or l'expérience courante montre que les horloges des ordinateurs n'ont pas une fiabilité suffisante. Par conséquent, si l'horloge du serveur est utilisée pour dater les actions qui doivent l'être, comme la remise des offres, et en indiquer l'heure dans une preuve de dépôt adressée à l'émetteur, cette horloge doit être surveillée, et remise à l'heure chaque fois que nécessaire. Il faut de plus que cette heure soit

affichée sur les pages web que consultent les entreprises, pour qu'elles puissent déceler d'éventuels décalages et en tenir compte. Toutes précautions doivent bien sûr être prises pour être en mesure de démontrer en cas de litige que cette horloge était exacte quand la preuve de dépôt a été émise.

3.5 Précautions diverses

Il peut arriver que les **fichiers** à échanger dans une procédure de marchés publics soient **très volumineux.** Les textes prévoient d'ailleurs ce cas, la personne publique pouvant permettre de n'envoyer avant l'heure limite que la signature des documents, un délai supplémentaire étant accordé pour les documents eux-mêmes (système du double envoi) à l'initiative de la PRM, cette possibilité devant être précisée dans le règlement de la consultation.

Ces possibilités ne dispensent cependant pas la personne publique de s'assurer que les débits disponibles pour transmettre les documents sont adaptés aux volumes à transmettre, pour que l'accès n'en soit pas refusé en cas d'engorgement. De même les entreprises qui ont des fichiers volumineux à transmettre doivent s'assurer que leur connexion offre bien un débit suffisant, et prendre en compte le risque qu'un envoi volumineux ne soit acheminé que lentement.

Au cas où la plate-forme constaterait que ses connexions à internet approchent de la saturation (et a fortiori si elle est indisponible, ou si la plate-forme elle-même est indisponible), il est nécessaire qu'elle en informe les PRM dont elle héberge les procédures de marché, qui prendront alors les mesures nécessaires, comme de prolonger le délai de remise des offres (cf. annexe 7)

Enfin, et bien qu'il ne s'agisse pas uniquement de problèmes de sécurité, il est évident que les documents dématérialisés doivent être commodément lisibles par leur destinataire. La personne publique, notamment, doit donc les émettre dans un format couramment répandu, et spécifier dans quels formats elle acceptera les documents que lui adresseront les entreprises. Elle doit veiller à utiliser et proposer aussi, chaque fois qu'il en existe, des **formats** capables d'être **manipulés par des logiciels gratuits** raisonnablement répandus et de bonne qualité. Sur ce point le vade-mecum conseille d'ailleurs d'utiliser « des formats électroniques qui permettent de **figer ces documents dans un état donné** » : c'est en particulier les cas du format « portable document format » (pdf), que l'on peut créer et lire avec des logiciels gratuits.

4 Mesures de sécurité à prendre pour les marchés dématérialisés

- d'une part des mesures spécifiques à la dématérialisation des marchés publics. Ces mesures spécifiques sont indiquées dans le paragraphe « Mesures de sécurité par type d'acteur » ci-après ;

- d'autre part les mesures techniques et organisationnelles minimales à prendre pour tout site internet mis en ligne, comme pour l'utilisation de serveurs informatiques et d'ordinateurs personnels. Ces mesures représentent le minimum, faute de quoi les systèmes informatiques sont exposés à toutes les malveillances ordinaires que l'on constate quotidiennement sur internet. Compte tenu des enjeux, d'autres mesures générales sont suggérées, utiles et qui peuvent, pour certaines organisations déjà bien structurées et équipées du moins, être prises sans gêne ni surcoût significatifs.

Les mesures proposées ci-après s'efforcent de constituer un ensemble équilibré et on indique les raisons pour lesquelles il est nécessaire de les prendre, ainsi que la sévérité des menaces qu'elles peuvent contribuer à éviter ou à atténuer. Elles ne prétendent être ni suffisantes, car il subsiste toujours un risque résiduel qu'il faut gérer, ni même toutes nécessaires dans toutes les situations : il faut donc, pour chaque cas particulier, apprécier si les raisons de prendre une des mesures qui sont indiquées existent bien – sinon on peut se dispenser de cette mesure – et si l'efficacité de cette mesure est bien cohérente avec la sévérité des menaces envisagées – sinon soit il faut la renforcer, soit on peut envisager de l'alléger.

4.1 L'exposé de ces mesures s'appuie sur une architecture générique du système

Ce dernier comprend :

- un serveur et ses logiciels[5] (l'ensemble étant appelé « plate-forme ») auxquels accèdent aussi bien la personne publique pour y déposer ses documents (AAPC, règlement de consultation, dossier d'appel à candidatures, DCE) et prendre connaissance des candidatures et des offres, que les entreprises pour consulter, télécharger les documents émis par la personne publique, remettre de façon sécurisée leurs candidatures et leurs offres ; la personne publique peut réaliser et mettre en œuvre cette plate-forme elle-même, probablement en achetant un progiciel qui assure les fonctions nécessaires ; elle peut aussi s'adresser à un prestataire qui assure ce service au profit de multiples autres clients ;

- un moyen pour la personne publique de faire connaître ses décisions aux entreprises (admises ou non à concourir, attributaires du marché ou non); le courrier électronique simple doit être accompagné d'une demande explicite d'accusé de réception (cf. annexe 13) : on peut également soit recourir à une publication sur le serveur qui assure cette traçabilité, avec contrôle d'accès si les informations affichées ne doivent pas être publiques, soit utiliser un courrier électronique recommandé, soit des procédures manuelles;

- un moyen pour l'entreprise et la personne publique de correspondre, par exemple pour le dialogue compétitif ; ici encore, pour les raisons évoquées ci-dessus, les mêmes précautions sont à prendre avec le courrier électronique;

- des moyens d'archivage pour la personne publique ;

- des moyens de bureautique ordinaires pour les entreprises et la personne publique.

4.2 Rôles[6] des personnes impliquées dans la procédure

- pour la personne publique : d'une part celles dont le rôle est défini par les textes (PRM, membres de la commission d'appels d'offres) et d'autre part les personnes mandatées pour établir et faire approuver les documents, négocier avec les entreprises (experts techniques, directeurs de projet, services achats etc.). Ces personnes peuvent ne pas être les mêmes pour toutes les consultations que mène la personne publique. Comme dans le cas des procédures manuelles, certains des documents et correspondances avec les entreprises que traitent ces personnes sont confidentiels et leur accès doit donc être réservé aux seules personnes autorisées. Tous ces documents et correspondances doivent être intègres, et leur origine, voire leur date d'émission doivent être connues de façon fiable ;

- de même, pour l'entreprise, il y a d'une part la personne dont la signature engage l'entreprise pour la consultation et d'autre part les personnes qu'elle mandate pour divers contacts avec la personne publique. La plupart des correspondances qu'adresse l'entreprise à la personne publique et des actions qu'elle mène (par exemple, même dans les cas où le DCE n'est pas confidentiel, le fait qu'une entreprise donnée télécharge ce DCE manifeste qu'elle s'intéresse au marché, et ne doit donc pas être connu de ses concurrents) sont confidentielles ; de plus les correspondances qu'elle adresse à la personne publique doivent être intègres et leur origine voire leur date d'émission doivent aussi être connues de façon fiable ;

[5] Comme indiqué ci-dessus, d'autres solutions techniques peuvent être mises en œuvre ; dans ce cas, il appartient aux personnes publiques et aux entreprises d'adapter les mesures proposées.

[6] Il s'agit de rôles et non de personnes physiques identifiées; selon l'organisation en place chez la personne publique et dans l'entreprise, une même personne peut en effet tenir plusieurs rôles.

- pour les deux parties il y a les informaticiens, qu'ils soient des employés de ces parties ou des sous-traitants (cas notamment du recours par la personne publique à un prestataire pour opérer la plate-forme). Ils ne doivent pas prendre connaissance des documents confidentiels ni des actions confidentielles concernant la procédure, non plus, a fortiori, que des éléments secrets mis en œuvre (clés de chiffrement, d'authentification, mots de passe par exemple). Or il se peut que, de par la conception du système, ils puissent et même doivent (par exemple pour analyser d'éventuels incidents) avoir accès à ces données confidentielles : il est donc indispensable que des consignes claires soient données aux informaticiens, quant aux circonstances dans lesquelles ils peuvent être autorisés à accéder à ces données, et qu'ils s'engagent à ne pas les divulguer. Il est nécessaire de plus que les accès éventuels à ces données soient journalisés de façon fiable. Si la personne publique recourt à un prestataire, elle doit connaître les circonstances qui justifieraient l'accès aux données confidentielles, et les modalités de ces accès éventuels ; de toutes façons un engagement de confidentialité doit être obtenu du prestataire, appuyé par les mesures techniques et organisationnelles qu'il prend pour tenir cet engagement (cf. annexe 10).

Les mesures indiquées ci-après restent, par nécessité, assez générales : il est donc nécessaire de les préciser pour les adapter à chaque cas particulier. De plus, il est bien évident qu'il ne suffit pas d'édicter ces règles générales et de s'en remettre à la bonne volonté des intervenants pour les appliquer. Dans chaque entité (entreprise, personne publique, prestataire éventuel) **une personne** doit donc être **chargée de la sécurité** des systèmes d'information ; son rôle est de préciser les consignes décrites ci-après, d'organiser la sensibilisation des intervenants à la sécurité, de veiller à l'application des consignes, de se faire rendre compte des incidents éventuels et d'en tirer les enseignements, tout ceci pour être en mesure de **démontrer**, en cas de litige, **qu'il n'y pas eu de négligence grave**.

4.3 Mesures de sécurité par type d'acteur

4.3.1 Mesures de sécurité concernant l'entreprise

- acquérir un certificat PRIS niveau 2 au moins auprès d'un prestataire référencé, à l'usage exclusif de la personne qui signera la candidature et l'offre (ce certificat de signature ne doit pas être utilisé pour le chiffrement) pour les marchés formalisés ;

- vérifier, en accédant à la plate-forme, que le certificat de cette plate-forme est bien celui que le prestataire a publié (voir « mesures à prendre par la plate-forme » ci-après) ;

- signer (par son certificat) puis chiffrer (par les moyens que la personne publique aura mis à sa disposition) sa candidature et son offre, après s'être assurée que ces pièces ne contiennent pas de virus (si un antivirus **à jour** est installé sur l'ordinateur utilisé, cette vérification peut être automatique) ;

- pour les échanges avec la personne publique qui devraient se faire par courrier électronique (c'est à dire dans le cas où la plate-forme n'offre pas un autre service qui permet ces échanges) , utiliser de préférence les courriers recommandés avec accusé de réception, et les signer s'ils sont émis par la personne titulaire du certificat ;

- prendre toute mesure pour préserver en interne la confidentialité des fichiers (cf. § «consignes générales, précautions particulières pour les marchés publics ci-après) ;

- veiller à ce que les moyens d'authentification nécessaires pour accéder au serveur (mots de passe par exemple) soient disponibles pour les personnes qui en ont besoin, et pour elles seules; en particulier, les certificats de personne ne doivent être utilisés que par leur seul titulaire ;

- conserver tous les fichiers afférents à la procédure et susceptibles d'être utiles en cas d'incident (fichiers téléchargés, informations déposées sur la plate-forme, certificats de dépôt et accusés de réception des courriers électroniques, candidatures et offres signées…) ;

- prendre les précautions nécessaires pour que les fichiers volumineux qu'elle adresse à la personne publique lui parviennent dans les délais nécessaires, que le système du double envoi (cf. vade-mecum juridique, § 9.6) soit ou non autorisé par la personne publique.

4.3.2 Mesures de sécurité concernant la plate-forme

Ces mesures s'appliquent, que la plate-forme soit opérée par un prestataire ou par des employés de la personne publique.

- la **plate-forme doit être sécurisée** (cf. § « consignes générales » ci-après : pare-feu, système de détection d'intrusion, exploitation des fichiers journaux de ces dispositifs, anti-virus…) ;

- elle doit être pourvue d'un **certificat de serveur** qui permet de l'authentifier auprès des entreprises qui la consultent, et de signer les documents qui y sont accessibles ; ce certificat doit être publié d'une façon infalsifiable et commodément accessible, par exemple dans la presse; la plate-forme doit donc indiquer sur quel support il est possible de vérifier son certificat ; ceci afin d'éviter que les entreprises ne soient, par malveillance, amenées à s'adresser à un autre site se faisant passer pour la plate-forme ;

- elle doit assurer un **contrôle anti-virus** des fichiers non chiffrés qu'elle reçoit, et prévenir l'émetteur des fichiers porteurs de virus ;

- garantir **l'intégrité et l'origine des documents** qui lui sont confiés ;

- elle doit **horodater et tracer** de façon fiable et opposable toutes les actions où elle intervient (et, si elle ne recourt pas à un serveur d'horodatage, afficher sur le site l'heure qu'elle détient) ;

- elle doit assurer un contrôle d'accès aux informations qu'elle détient, en lecture si elles sont confidentielles et en écriture si leur intégrité doit être préservée ;

- elle doit fournir les **clés de chiffrement et de déchiffrement**, en garantir la qualité ainsi que la confidentialité de la clé de déchiffrement, confidentialité qui doit être totale jusqu'à ce qu'elle la remette à la PRM, et vis à vis de toute autre personne après ;

- elle doit également **séquestrer** cette clé de déchiffrement, pour être en mesure d'en fournir une copie en cas de besoin, par exemple si la PRM perd ou endommage la clé qui lui a été remise ; ce séquestre doit être fait de façon que la confidentialité des clés soit absolument préservée ;

- elle doit fournir un mécanisme qui permette de garantir que les candidatures et les offres jugées irrecevables n'ont pas été ouvertes ;

- elle doit 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, ni rendu momentanément indisponible ;

- être 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 ;

- elle doit garantir qu'aucune **information confidentielle** (offres et candidatures, mais aussi liste des entreprises candidates, retenues, qui ont répondu, échanges avec les entreprises…) qui lui a été confiée ne sera divulguée par sa faute ; cette garantie peut s'obtenir par des mesures techniques uniquement, c'est le chiffrement s'il est mis en œuvre de telle façon que les informaticiens ne disposent pas de la clé de déchiffrement (ce doit être impérativement le cas pour les candidatures et

les offres) ; pour les informations que la plate-forme doit détenir en clair, il faut y adjoindre des mesures organisationnelles, en assurant notamment le contrôles des accès de son personnel aux moyens informatiques (qui doivent être journalisés), en prenant des engagements de confidentialité ; les cas où les informaticiens devraient avoir accès à ces informations (correction d'incidents par exemple) doivent être prévus et justifiés, et ces accès doivent être également journalisés ;

- elle doit assurer la **confidentialité en transmission** des informations qu'elle échange avec les entreprises et la personne publique (un chiffrement par le protocole SSL, « secure socket layer », est en général adapté pour ce faire ;

- elle doit assurer une **disponibilité de niveau « fort »** (durée d'indisponibilité inférieure à deux heures) comme indiqué ci-dessus, au moins aux périodes de remise des candidatures et des offres, et prévenir les PRM qu'elle héberge en cas d'indisponibilité (cf. annexe 7) ;

- elle doit disposer de raccordements à internet de **débit suffisant** face au volume des fichiers qu'elle recevra et émettra, et prévenir les PRM qu'elle héberge au cas où ces raccordements approchent de la saturation ;

- afficher sur son site sa **politique de sécurité**, pour que les entreprises connaissent avec quel soin seront traités les documents qu'elles lui transmettront.

4.3.3 Mesures de sécurité concernant la Personne responsable des marchés (PRM) et les acheteurs

- les **personnes** intervenant dans la procédure doivent être sensibilisées aux risques que présentent l'informatique et internet et **formées** à l'utilisation des outils informatiques à mettre en œuvre et à leur **sécurité** (par exemple conduite à tenir en cas d'incident);

- ces personnes doivent être **identifiées**, et leur rôle précisé avec 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 évènements…). Il est nécessaire de **contrôler ces accès**, pour éviter que d'autres personnes interviennent à tort : elles 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 ;

- le **règlement de la consultation** doit indiquer les formats de fichier qu'acceptera la personne publique, les modalités selon lesquelles les entreprises transmettront leurs candidatures et leurs offres, et notamment la façon de les chiffrer, et les modalités d'échanges avec les entreprises. Pour ceux de ces **échanges** qui devraient se faire par messagerie électronique, il faut demander explicitement un accusé de réception ;

- **l'ouverture des candidatures** et des offres doit se faire de telle façon qu'il puisse être démontré que les précautions ont été prises pour :

    - éviter leur contamination par les ordinateurs de la personne publique au cours de cette opération (cf. annexes 5 et 6, « Virus et antivirus » et «Traçabilité de la décontamination des offres à l'ouverture ») ;
    - attester que pour celles, porteuses de virus, qu'il aurait été possible de réparer et décidé de ne pas rejeter, les seules modifications proviennent de la mise en œuvre de l'anti-virus ;
    - que les candidatures et offres jugées irrecevables (par exemple parce que reçues hors délai) n'ont pas été ouvertes (si du moins le service fourni par la plate-forme est jugé insuffisant) ;

- s'assurer que tous les **fichiers** nécessaires restent **disponibles**, même en cas de panne informatique qui endommagerait les copies de travail, donc veiller à ce qu'ils soient sauvegardés sur des supports externes (cassettes, cédérom, etc.) conservés en lieu sûr ;

- **archiver** tous les documents de façon opposable, avec les signatures qu'ils comportent, ainsi que l'indication que ces signatures étaient valables quand elles ont été apposées ; un archivage de ces données sur cédérom peut suffire pendant quelques années (cf. annexe 8).

4.3.4 Mesures de sécurité concernant les informaticiens de la personne publique (autres que ceux qui administrent une plate-forme opérée en interne)

- mettre en place les procédures et les outils nécessaires pour que la personne publique 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.) ;

- si la personne publique acquiert un **progiciel**, les informaticiens chargés du choix doivent s'assurer que le progiciel remplit bien les fonctions de sécurité indiquées ci-dessus comme nécessaires pour la plate-forme, et qu'il a les garanties de **pérennité** (par exemple le séquestre près d'un tiers du logiciel et de tous les éléments nécessaires pour en assurer la continuité en cas de défaillance de l'éditeur) , **maintenabilité** et **réversibilité** nécessaires (cf. annexe 11), et déterminer quelles **responsabilités** l'éditeur accepte de prendre en cas de dysfonctionnement de son produit ;

- si la personne publique recourt à un **prestataire** qui opère une plate-forme d'achats dématérialisés, elles doivent de plus obtenir les engagements de confidentialité mentionnés à propos de la plate-forme ; le prestataire doit également indiquer comment il pourrait assurer l'achèvement des affaires en cours s'il devait rencontrer des difficultés (assurances, repli sur un autre prestataire etc.) et donner les assurances nécessaires quant à la sécurité de la prestation en décrivant (cf. annexe 10) :

    - sa politique de sécurité ;
    - la qualification des solutions de sécurité ;
    - la gestion du changement et validation des mises à jour techniques ;
    - la gestion des accès logiques et détection des activités non autorisées ;
    - la surveillance des performances ;
    - la gestion des incidents ;
    - les procédures de sauvegardes des données et des configurations ;
    - les procédures assurant la continuité des services ;
    - les audits du niveau de sécurité auxquels il fait procéder ;
    - son plan de continuité des activités ;
    - ses méthodes de surveillance des vulnérabilités et des menaces potentielles.

4.4 Consignes générales

4.4.1 L'utilisation de moyens informatiques, surtout s'ils sont raccordés à internet, exige des précautions minimales :

- le raccordement à internet doit être filtré par un pare-feu équipé d'un antivirus ;

- les postes de travail doivent impérativement être équipés d'un anti-virus tenu à jour quotidiennement ; pour une meilleure efficacité, cet antivirus ne doit pas être le même produit que celui du pare-feu ;

- ils doivent également être équipés aussi d'un produit de détection et d'éradication des espiogiciels (appelés aussi « spywares » : ce sont programmes qui renvoient à l'extérieur des informations qui ne devraient pas sortir furtivement du poste), également tenu à jour ;

- les logiciels doivent être paramétrés de façon sûre (options par défaut examinées pour juger de leur intérêt et de leur dangerosité, options dangereuses désactivées) ;

- les vulnérabilités publiées[7] sur les logiciels utilisés doivent être régulièrement corrigées, en appliquant rapidement les correctifs proposés par l'éditeur ;

- les utilisateurs doivent être sensibilisés aux risques que présente l'utilisation de leur ordinateur, et appliquer des règles de comportement prudent : la plus évidente est de se méfier des messages électroniques bizarres, dont les pièces jointes sont généralement porteuses de virus, même si ces messages semblent provenir d'une personne connue ; beaucoup d'entreprises et d'administrations n'autorisent pas leurs employés à accéder à tous les sites internet, ceci pour éviter qu'ils ne perdent de temps en consultations extra-professionnelles, voire qu'ils consultent depuis leurs postes de travail des sites répréhensibles (racisme, pédophilie…), discutables (pornographie…) ou susceptibles de contaminer leur ordinateur; il faut également interdire l'importation de logiciels et de fichiers qui ne seraient pas indispensables aux activités professionnelles; en particulier toute utilisation sur une de ses machines de logiciels qui n'ont pas été acquis légalement expose l'entreprise ou la personne publique propriétaire de ces machines à des poursuites pénales ;

- une sauvegarde régulière des fichiers importants est nécessaire, pour ne pas perdre ces fichiers en cas d'incident (matériel ou logiciel) sur l'ordinateur ; pour les fichiers du poste de travail, cette opération peut être faite par l'utilisateur lui-même, qui doit donc disposer des moyens nécessaires (graveur de cédérom, clé USB, cassette…), ou sur le serveur de fichiers, s'il existe ; pour les fichiers du serveur, il revient aux administrateurs de ce serveur de la mettre en œuvre ;

- 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 ;

- les utilisateurs doivent pouvoir recourir à une assistance technique dans leurs opérations, qui les aide aussi à traiter les éventuels incidents et à en limiter la propagation dans le reste du réseau ;

- l'accès au poste de travail doit être protégé, au minimum par un mot de passe et en fermant à clé le local où se trouve le poste;

- pour éviter les malveillances internes, ou même les simples indiscrétions, les postes individuels doivent être équipés d'un pare-feu individuel ; il est recommandé de plus de chiffrer[8] les fichiers sensibles, en particulier s'ils sont stockés sur un serveur de fichiers et ne doivent pas être lus par les informaticiens qui administrent ce serveur ;

- puisque le courrier électronique ne présente aucune garantie de sécurité, tous les courriers présentant une certaine confidentialité doivent être chiffrés avant de circuler sur des moyens non contrôlés, internet bien sûr, mais aussi le réseau interne si les risques d'indiscrétion interne ne sont pas totalement écartés ;

- 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.

[7] Voir notamment le site du Premier Ministre http://www.certa.ssi.gouv.fr/site/index2.htm#avis

[8] il existe des produits de chiffrement gratuits de bonne qualité, souvent adaptés à un usage individuel; d'autres produits, payants ou gratuits comme GPG, sont mieux adaptés à des déploiements de quelque importance.

4.4.2 La sensibilité des marchés publics requiert une attention particulière dans l'utilisation des moyens informatiques :

- les fichiers présentant des exigences de disponibilité, notamment pour des raisons juridiques (candidatures, propositions…), doivent être systématiquement sauvegardés dès leur réception par la PRM[9], leur perte pouvant conduire à l'annulation de la procédure ;

- toutes les précautions doivent être prises pour que les fichiers confidentiels (comme par exemple les propositions après leur déchiffrement) ne soient pas divulgués ; comme indiqué ci-dessus, cela peut exiger, dans le cas où le risque d'indiscrétion interne n'est pas totalement écarté, de protéger l'accès aux postes des personnes qui les traitent voire de les rechiffrer sur ces postes et/ou le serveur de fichiers où ils sont stockés ; il est alors recommandé, de plus, d'équiper les postes de travail d'un pare-feu individuel ;

- comme indiqué ci-dessus, la machine où seront ouverts les fichiers transmis par les entreprises doit être équipée d'un antivirus parfaitement à jour, qui sera systématiquement exécuté juste avant l'ouverture des offres, pour s'assurer qu'elle ne risque pas de contaminer ces offres ; elle doit être protégée au moins comme les autres postes où seront traités les fichiers confidentiels (voir annexe 6) ;

- l'accès aux moyens permettant d'effectuer les opérations de sécurité, comme la signature et le chiffrement/déchiffrement, doit être protégé, pour empêcher qu'ils soient utilisés indûment ;

- comme pour les procédures manuelles, les personnes devant avoir accès aux informations sensibles doivent être identifiées, leurs rôles et droits précisés et elles doivent être dotées de moyens d'accéder à ces informations (ce qui serait le cas par exemple si celles-ci étaient stockées sur un serveur partagé avec d'autres utilisateurs étrangers à la procédure).

[9] Ou au moins dès qu'ils ne lui sont plus accessibles sur la plate-forme d'achat. Outre les exigences de disponibilité qu'elle doit satisfaire, cette plate-forme doit bien sûr garantir qu'aucun fichier qu'elle aura reçu ne peut être détruit ni endommagé pendant la période où le prestataire s'est engagé à le conserver. Pour les fichiers qui n'existent sur la plate-forme que sous forme chiffrée, comme les offres, la PRM, qui a reçu les moyens de déchiffrement doit veiller à ce que ces moyens soient disponibles aussi longtemps que nécessaire.

ANNEXE 1 : comment mettre en place un service de dématérialisation des achats

1. Introduction

Afin de pouvoir dématérialiser ses procédures de passation des marchés publics, une personne publique a deux possibilités :

- soit elle externalise la solution de dématérialisation (1) ;
- soit elle internalise la solution de dématérialisation (2).

2. Recourir à un service de dématérialisation fourni par un prestataire extérieur

Dans cette hypothèse, la personne publique confie à un prestataire la mise à disposition d'une solution de dématérialisation à destination des candidats aux marchés publics. La personne publique ne se charge donc pas elle-même du service. Elle va faire appel à un prestataire extérieur pour couvrir ses besoins.

Les obligations du prestataire seront définies dans les documents du marché dont il est titulaire. Il convient donc à la personne publique d'évaluer correctement ses besoins et les prestations qu'elle désire.

Ainsi, si elle considère qu'une charte d'utilisation est souhaitable, elle a intérêt à exprimer cette exigence dans son cahier des charges.

Indépendamment des obligations contractuelles, certaines démarches sont légalement indispensables à la mise en place d'un service de dématérialisation. Ces démarches sont réparties entre la personne publique et le prestataire.

3. Les démarches à accomplir par la personne publique

La personne publique est considérée au titre de la loi informatique et liberté comme le responsable du traitement. C'est donc elle qui doit se plier à l'accomplissement des formalités déclaratives. Toutefois, la personne publique peut demander (il faut le prévoir dans le cahier des charges) à son prestataire de remplir certains champs du formulaire d'autorisation, dans la mesure où c'est lui qui a en partie la charge du traitement des informations.

A noter[10] que la CNIL entend très prochainement faire application des dispositions de la nouvelle loi Informatique et Libertés pour simplifier les procédures déclaratives des organismes publics dans le cadre de la mise en place de plates-formes de dématérialisation des marchés publics. Dans l'attente de ces mesures d'allégement des formalités préalables, les organismes publics n'ont pas à adresser de déclaration à la CNIL. Bien entendu, la simplification apportée aux procédures déclaratives ne dispense pas de l'obligation de respecter les règles de fond de la loi du 6 janvier 1978.

La personne publique doit également vérifier que le prestataire a rempli ses obligations déclaratives auprès de la DCSSI et que la solution du prestataire remplit bien les obligations réglementaires en matière de confidentialité, d'accessibilité à tous, de sécurité, etc. (cf. mesures de sécurité à appliquer par la plate-forme, § 4.2.2 du guide).

[10] http://www.cnil.fr/index.php?id=1743&news[uid]=225&cHash=e866a86ff7

Bien qu'il ne s'agisse pas d'obligations légales, il est prudent que la personne publique vérifie que le prestataire a souscrit une assurance suffisante pour couvrir les risques liés à son activité, et qu'elle édicte dans son règlement de consultation une charte d'utilisation de la plate-forme, pour lier les candidats aux conditions d'utilisation de cette plate-forme. Si c'est la plate-forme qui dispose elle-même d'une telle charte, elle doit veiller, lorsqu'elle y apporte des modifications, à laisser accessibles les versions antérieures sur lesquelles se sont appuyées les entreprises dans leurs démarches : il ne serait pas normal en effet de leur opposer un texte qui n'aurait été publié qu'après ces démarches.

4. Les démarches que doivent accomplir les prestataires

- Disposer d'une assurance suffisante couvrant les risques liés à son activité de prestataire de service de dématérialisation.

- Déclarer à la DCSSI la fourniture de clé de chiffrement à des fins de confidentialité.

- Etre à jour au niveau de ses déclarations CNIL (ex : pour ses fichiers commerciaux, son site internet, etc.). Toutefois, le prestataire n'a pas à déclarer le traitement des fichiers de données nominatives faisant l'objet d'un traitement informatique lors de l'utilisation de la solution de dématérialisation. Il est considéré au titre de l'article 35 de la loi n°78-17 dite « informatique et liberté » comme un « sous-traitant ». C'est au responsable du traitement, c'est à dire à la personne publique, qu'il incombe d'accomplir les obligations déclaratives (cf. ci-dessus, obligations de la personne publique).

- Etablir des politiques de sécurité afin de rendre public ses engagements sur les différents aspects de la sécurité (horodatage, confidentialité, etc.).

5. Développer une plate-forme internalisée

Que ce soit le personnel de la personne publique ou un prestataire extérieur qui construise la plate-forme de dématérialisation, la personne publique est responsable de l'outil de dématérialisation internalisé. Ainsi, c'est à elle qu'il revient d'accomplir certaines démarches (a) et de gérer l'utilisation de la plate-forme de dématérialisation (b).

5.1 Les démarches préalables au développement d'une solution de dématérialisation

La personne publique doit examiner s'il est nécessaire de souscrire une assurance ou d'étendre son assurance de telle manière à couvrir les risques liés à un dysfonctionnement de la solution de dématérialisation (ex : indemnisation d'un candidat ayant vu son offre rejetée comme trop tardive du fait d'une erreur d'horodatage).

- Faire une déclaration à la DCSSI relativement à l'utilisation de moyen de cryptographie à des fins de confidentialité. En effet, une des obligations posées par le décret 2002-692 du 30 avril 200 portant application du 1° et 2° de l'article 56 du code des marchés consiste à préserver la confidentialité des offres ou des candidatures transmises. Techniquement, cela suppose l'utilisation de clés de chiffrement à des fins de confidentialité. Or, la fourniture à autrui de solutions de chiffrement à des fins de confidentialité est soumise à une obligation de déclaration auprès des services de la DCSSI (les articles 30 et 31 de la loi sur la confiance dans l'économie numérique soumettent la fourniture ou les prestations de cryptologie à des fins de confidentialité à une déclaration auprès des services du Premier ministre. Les décrets d'application n'ayant pas été pris, c'est l'ancien régime de déclaration au près de la DCSSI qui s'applique)

- Demander l'autorisation préalable de la CNIL pour le traitement des fichiers de données nominatives utilisés dans le cadre de la dématérialisation de la procédure de passation (ex : gestion du fichier de retrait des DCE et de dépôt des offres et des candidatures) et éventuellement pour la création d'un site internet lié à la plate-forme dans la mesure où celui-ci traite ou diffuse des données

nominatives (ex : pour créer un identifiant et un mot de passe, l'internaute doit remplir un formulaire de collecte des données où son nom et son prénom sont demandés). Comme indiqué ci-dessus (§ 1.1), la CNIL entend très prochainement faire application des dispositions de la nouvelle loi Informatique et Libertés pour simplifier les procédures déclaratives des organismes publics dans le cadre de la mise en place de plates-formes de dématérialisation des marchés publics. Dans l'attente de ces mesures d'allégement des formalités préalables, les organismes publics n'ont pas à adresser de déclaration à la CNIL. Bien entendu, la simplification apportée aux procédures déclaratives ne dispense pas de l'obligation de respecter les règles de fond de la loi du 6 janvier 1978.

- Si la solution de dématérialisation est liée à un site internet, il faut déposer le nom de domaine auprès de l'AFNIC (ex : pour les noms de domaine en .fr) ou de l'ICANN (ex : pour les noms de domaine en.com) afin que l'accès au site soit facilité.

5.2 Gestion de l'utilisation de la plate-forme de dématérialisation

Mesures obligatoires :

Si la plate-forme de dématérialisation est associée à un site internet (proposant des services autres qu'un système de correspondance privée), il faut publier « l'ours du web », c'est-à-dire le nom du directeur de publication, la dénomination et les coordonnées de la personne publique, les coordonnées et la raison social de l'hébergeur (Loi 2000-719 du 1er août 2000 modifiant la loi du 30 septembre 1986 relative à la liberté de la communication).

L'outil de dématérialisation étant amené à traiter des données nominatives, il faut informer les utilisateurs des champs obligatoires et de leurs droits (droit d'accès et de modification) sur les formulaires de collecte des données. Cela implique également d'être en mesure de gérer les demandes d'accès et de modification émanant des utilisateurs notamment en donnant aux utilisateurs les coordonnées du service à contacter pour procéder à l'accès et à la modification des données.

Bonnes pratiques :

Afin d'éviter et de limiter les contentieux avec les utilisateurs de la solution de dématérialisation, il peut être bon de contractualiser les rapports entre la personne publique donnant accès à l'outil de dématérialisation et l'utilisateur de l'outil. Ainsi, il est utile de rédiger une « charte d'utilisation des services » qui devra être acceptée par les utilisateurs.

Afin d'être conforme à la pratique des autorités d'horodatage et de confidentialité, la personne publique doit établir des politiques de sécurité (politique d'horodatage, politique de confidentialité, sauvegardes, réactions aux incidents, contrôles d'accès, mesures en cas d'indisponibilité etc.), ce qui permet aux utilisateurs de connaître le niveau d'engagement technique de la personne publique.

ANNEXE 2 : signature électronique et certificat : quelques points clés par la Délégation aux systèmes d'information

Ce document a été rédigé dans le seul but d'aider les utilisateurs de signatures électroniques et de certificats à s'initier à ces techniques en leur fournissant quelques explications simples.

Il n'a pas pour objectif de se substituer à une formation, à des ouvrages ou à la documentation qui accompagne ces outils.

Il a un parti pris dans l'illustration qui repose sur l'outil de gestion *options internet* de Microsoft®[11]. Pour autant les informations fournies sont similaires dans tous les autres environnements et les explications sont les mêmes quels que soient les logiciels utilisés.

Enfin il peut comporter des erreurs qui pourraient être signalées à :
dsi@ finances.gouv.fr

1. La signature électronique et le certificat

La signature électronique permet de mettre en œuvre un certain nombre de fonctions indispensables à la sécurité des échanges sur l'internet.

Si ses concepts et sa mise en œuvre sont simples, il n'en va pas de même de son usage pratique qui demande un minimum d'apprentissage.

En outre utiliser convenablement des outils, et ceux-ci en particulier, nécessite de bien comprendre leurs conséquences afin d'engager sa responsabilité de façon consciente et opportune.

Cet obstacle franchi il n'en demeure pas moins que l'ultime difficulté sera toujours de pouvoir s'assurer que celui avec qui je traite (*eg.* : l'émetteur d'un message) est bien celui qu'il dit être (il a signé son message avec sa clé privée), puisque par construction sur l'Internet n'importe qui peut s'adresser à moi .

Bien entendu il est possible que je me fasse communiquer en face à face les éléments d'identification de chaque émetteur (ie : la clé publique), mais si j'ai des centaines de correspondants la limite est vite atteinte.

Il faudra donc avoir recours à un intermédiaire dont la fonction sera de me garantir que celui qui s'adresse à moi est bien celui qu'il dit être. Je vais donc devoir sous-traiter l'identification à un tiers de confiance qui me garantira que l'identité du porteur du certificat est vraie et que la clé privée pour signer est valide (celle qui est associée au certificat et donc au bon code secret).

En résumé, la signature ce sont les **outils techniques** qui peuvent être utilisés entre des internautes qui se connaissent a priori (ou dont les données ne sont pas importantes) alors que le certificat c'est la **confiance** qui permet des échanges entre des internautes qui ne se verront jamais ou dont les données ont de la valeur.

[11] Accès dans :
- l'environnement Microsoft Internet Explorer® avec la fonction Outils puis Options internet. Choisir l'onglet Contenu puis presser le bouton certificats.
- l'environnement MOZILLA© et NETSCAPE© avec la fonction Edition puis préférences. Choisir le panneau Certificats puis presser le bouton Gestion des certificats.

2. La signature

2.1 Intégrité, authentification, non répudiation et chiffrement sont les 4 services rendus par les outils

Intégrité

Le message émis arrive sans altération au destinataire. Dans le cas contraire le message est signalé comme ayant été modifié.

Authentification

L'émetteur est authentifié, c'est à dire que ce qu'il déclare être est exact, que l'origine du message ou de la transaction sont incontestables.

Non répudiation

Il est possible de prouver qu'un message a été envoyé par un émetteur précis et seulement par lui. Réciproquement celui qui a envoyé ce message ne peut en refuser la propriété.

Chiffrement

Le message clair est transformé en cryptogramme.

2.2 L'intégrité

Une partie du message est extraite (empreinte, ou hachage ou hasch, etc.) grâce à la fonction mathématique « hash »[12].

Cette empreinte est transmise avec le message dont il faut vérifier qu'il n'a pas été altéré. A la réception du message, et avec la même fonction, on prend une empreinte du message qui est comparée avec celle qui a été transmise. Si les deux empreintes sont identiques alors le message est intègre.

Pour s'assurer que l'empreinte elle-même est transmise de façon intègre (on pourrait remplacer le message et l'empreinte !) celle-ci est chiffrée avec la clé privée de l'émetteur (A). Elle sera déchiffrée avec sa clé publique par le destinataire.

Bien sur il est possible de se demander pourquoi prendre une empreinte plutôt que de chiffrer le message, ce qui rendrait le même service. Ceci tient au fait que le chiffrement est lent et que la taille des fichiers à chiffrer peut-être considérable.

La fonction hash restitue une empreinte qui est indissociable du document dont elle est extraite et qui est de longueur fixe et brève. Ainsi la durée du chiffrement est-elle toujours identique qu'elle que soit la taille du fichier à signer.

(Remarque : c'est le chiffrement de cette empreinte qui interdit parfois aux messages signés de franchir certaines passerelles de messageries car les pare-feux ne pouvant en extraire le contenu aux fins d'analyse, refusent le transfert).

[12] Les deux algorithmes les plus utilisés sont MD5 et SHA1. MD5 est jugé insuffisant.

2.3 L'authentification

A une clé A (privée) correspond une clé B (publique) et une seule, et réciproquement. Signer un message c'est lui joindre une empreinte de ce message chiffrée avec la clé privée A et qui de ce fait ne pourra être déchiffrée qu'avec la clé publique B.

Comme la clé B ne peut déchiffrer que ce qui a été émis par la clé A alors le message est bien émis par le détenteur de la clé privée A.

2.4 La non répudiation

Si je suis sur qu'un message a été signé par une clé privée A (et je peux en être sur puisque je détiens la clé publique B qui ne peut fonctionner qu'avec la clé privée A) alors le message n'a pu être émis que par celui qui utilise la clé A.

Bien sur il reste la question de savoir si celui qui l'utilise et qui s'authentifie est bien celui qu'il prétend être (le fait d'avoir la carte de paiement ne fait pas de moi son titulaire, il me faut aussi disposer du code) et cela c'est le rôle du **certificat.**

2.5 Le chiffrement

Le chiffrement avec des clés asymétriques a ceci de remarquable que ce qui est chiffré avec l'une des deux clés peut être déchiffré par l'autre (et bien sur par elle seulement !). C'est cette particularité qui est utilisée pour l'authentification : je chiffre l'empreinte avec ma clé privée – et je suis seul à pouvoir le faire- et le destinataire déchiffre avec ma clé publique – et tout le monde peut le faire.

Pour envoyer un message chiffré dont on veut s'assurer que seul le destinataire pourra le lire c'est le contraire : il faut utiliser sa clé publique pour chiffrer le message et lui seul avec sa clé privée pourra le rendre clair.

Ce qui rend le chiffrement périlleux c'est qu'en cas de perte de la clé privée il est alors impossible de déchiffrer les données qui sont alors perdues. C'est pourquoi les organisations ne fournissent cela qu'avec précautions. Certaines acceptent de « séquestrer » les clés de chiffrement mais ceci pose des questions juridiques et techniques fort complexes et dont les réponses sont très coûteuses.

2.6 La signature est personnelle, tout prêt est interdit…

Le certificat associe la signature (couple clés privée-publique) à une personne identifiée. Il le fait car sa délivrance est subordonnée à un minimum de contrôles d'identité dont le niveau fonde la confiance.

Ainsi les téléprocédures du MINEFI utilisent-elles uniquement des certificats délivrés en face à face et dont la qualité technique et le modèle économique ont fait l'objet d'audits.

Ce certificat pour être utilisé convenablement devrait toujours être associé à un code personnel, souvent appelé code PIN (« Personal identification number »). Ceci permet de procéder non seulement à l'**authentification**, *je dis qui je suis*, mais aussi à l'**identification**, *je suis qui je dis que je suis*, car je suis le seul à connaître le code.

On voit par là que la signature qui est placée sous le contrôle exclusif du titulaire ne peut être « prêtée » occasionnellement lors de congés ou d'absences à un secrétariat, un collaborateur ou un collègue.

La confiance serait profondément trahie et la réputation du titulaire détruite. En outre en cas de problèmes le titulaire serait pris dans une étreinte fatale :

- s'il reconnaît qu'il y a eu fausse signature il admet la rupture du contrat et il met la personne à laquelle il a confié le code dans une situation périlleuse puisque elle a fait un faux.

- s'il ne veut pas admettre la fausse signature alors il assume les conséquences de l'opération puisqu'il est réputé avoir lui-même réalisé l'opération.

En réalité dans la majorité des cas la question posée est celle de la gestion du temps. On « prête » ou on « confie » sa signature lorsqu'il n'y a pas eu de délégation de faite et car on est pris de court.

La délégation (momentanée ou permanente, limitée ou générale, etc.) n'est pas vraiment utilisée sauf dans des circonstances majeures, éloignement permanent, volumétrie excessive, car elle doit être anticipée et il est difficile et lent d'en informer ceux qui ont à en connaître (e*g.* : publication ou courrier préalable officiels, etc.). En outre les comportements actuels qui remontent à la nuit des temps administratifs permettent de s'en affranchir dans la majorité des cas.

Ce qui est donc essentiel c'est de définir à l'avance les règles d'usage et d'en assurer leur publication. Ceci facilite les pratiques et crée le climat de confiance nécessaire aux progrès de la dématérialisation.

2.7 La signature numérique rend-elle les mêmes services que celle qui est manuscrite ? Non ! Elle en donne plus !

Les procédures administratives nécessitent souvent que plusieurs personnes puissent signer le même document, successivement ou simultanément. Dans certains environnements seuls les courriers signés par deux responsables ont un plein effet.

Les outils de signature électronique permettent d'intégrer plusieurs signatures dans un document et garantissent la mise en évidence des modifications introduites par un signataire.

Ainsi il est possible d'avoir la certitude qu'un texte a bien été signé de façon identique par les signataires.

Ces outils travaillent soit avec des formats peu ou prou propriétaires (eg : Adobe®), soit avec des formats ouverts (eg : SXML).

De plus la vérification de ces signatures pourra avoir lieu bien des années plus tard sans qu'il soit besoin de reprendre contact avec leurs titulaires.

3. Le certificat

3.1 Son usage essentiel est de permettre l'identification

Qu'est-ce qu'un certificat ?
Selon le dictionnaire [13]: c'est un « écrit officiel ou dûment signé d'une personne compétente, qui atteste un fait ».

C'est un **« écrit… :**

il s'agit ici d'un fichier qui contient pour l'essentiel le nom du porteur et sa clé publique, ainsi que des informations de gestion (dates, algorithmes, etc.)

[13] Les définitions sont extraites du Petit Larousse illustré.

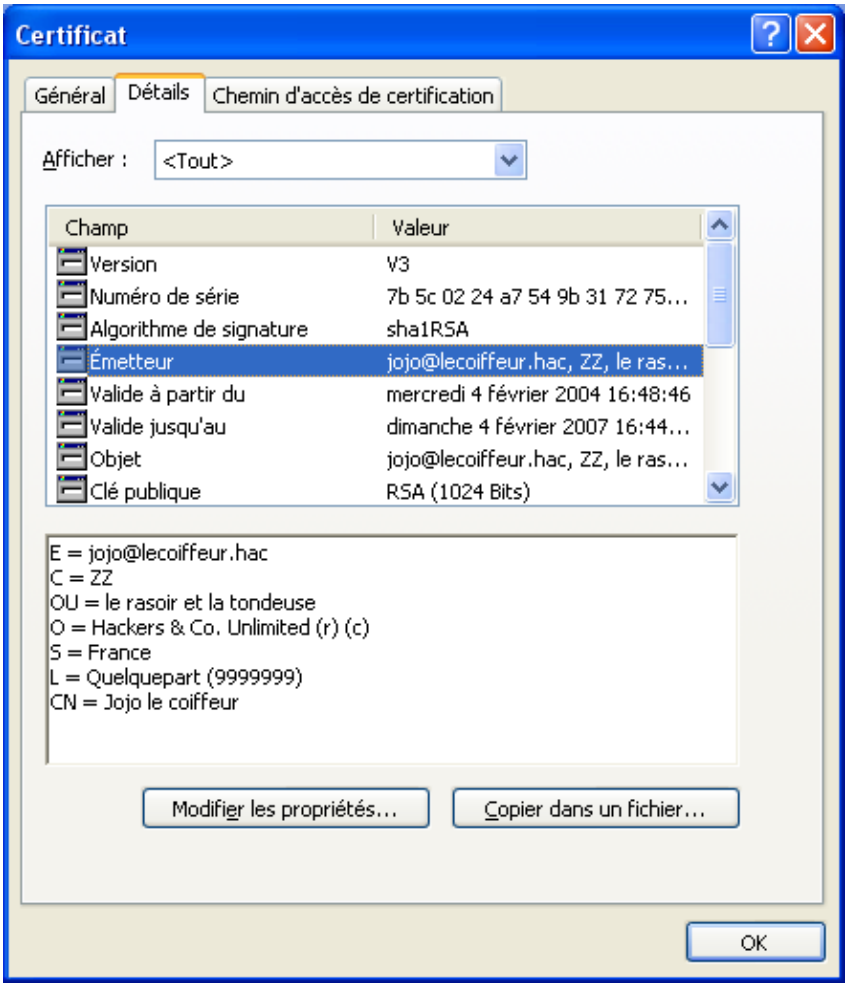
…officiel ou dûment signé d'une personne compétente… :
une organisation émettrice (personne compétente), ainsi la DPMA du MINEFI, la DREE, la DGI, Etc.

…qui atteste un fait :
le contenu du fichier (clé publique du porteur, nom, etc.) est bien celui qu'il doit être et que ce contenu appartient à la personne qui le revendique.

Qu'y trouve t'on ?

- le nom du porteur ;
- la clé publique du porteur de ce certificat ;
- les dates de validité ;
- l'organisation (si nécessaire) à laquelle appartient le porteur ;
- l'adresse où trouver les listes de certificats révoqués (LCR) ;
- le nom de l'entreprise de confiance, c'est à dire de l'autorité de certification, qui a émis ce certificat ;
- La signature de cette AC sur ce certificat ;
- On pourrait aussi y trouver la photographie du porteur ou du logo de l'entreprise.
- Etc.

3.2 Est-il est possible de voir et de lire le contenu d'un certificat ?



Le contenu de celui-ci n'inspire pas la plus grande confiance ?

Et pourtant l'essentiel n'est-il pas de s'assurer que ceux avec qui l'on va traiter (ou non !) sont bien identifiables et que le cas échéant il serait possible de les retrouver ?

Alors comment faire pour répondre à ces questions ?

- Il faut s'assurer que le certificat est utilisable ;
- il faut connaître l'autorité de certification qui a délivré le certificat et mesurer la confiance qu'il est possible de lui accorder, car c'est elle qui possède la preuve du lien entre la clé et son propriétaire de même qu'elle connaît son identité réelle, son domicile, etc.

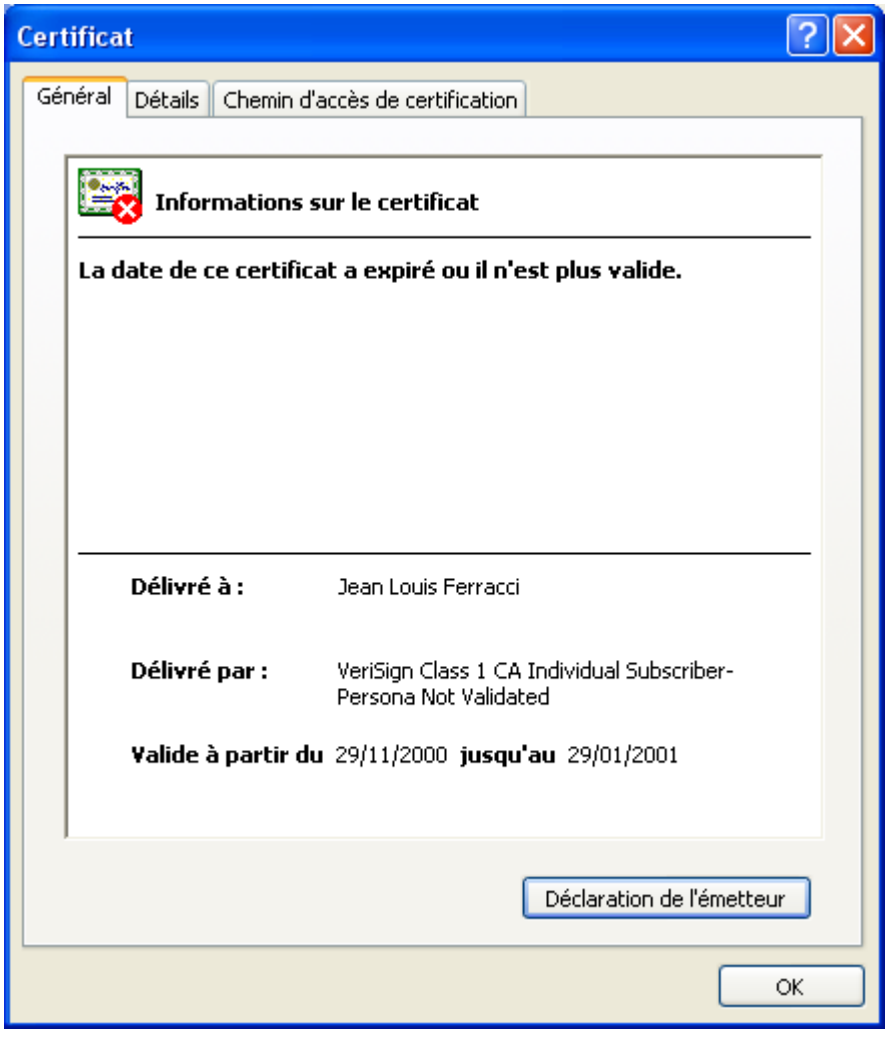
3.3 Comment vérifier un certificat ?

Trois éléments, au moins, du certificat doivent systématiquement être vérifiés :

- la validité ;
- la révocation ;
- l'usage.

3.4 La validité

L'outil de signature vérifie automatiquement la validité temporelle du certificat et donne un avertissement dans le cas où le certificat a expiré.



3.5 La révocation

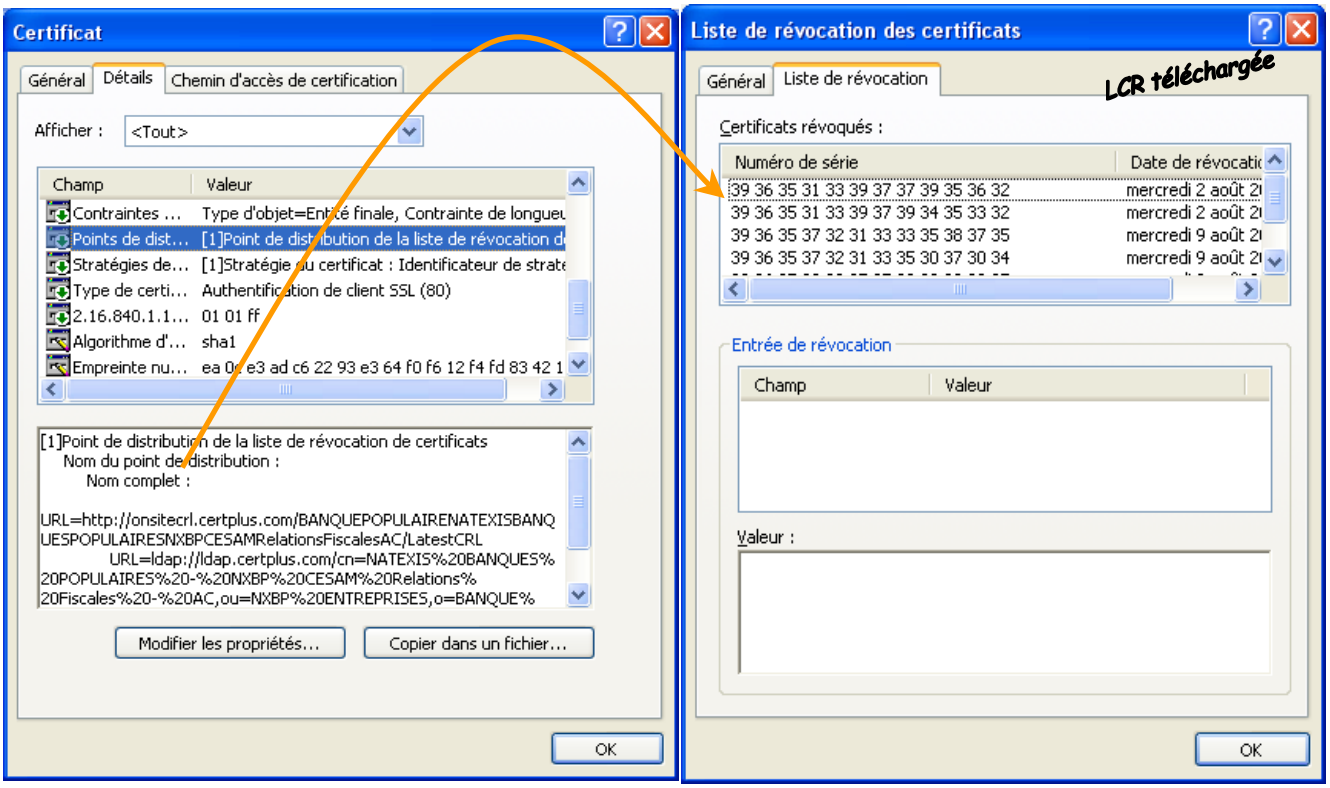
Le deuxième élément à vérifier est que le certificat est toujours utilisable.
Il faut s'assurer qu'il n'a pas été révoqué.

Cette révocation peut intervenir à la demande :

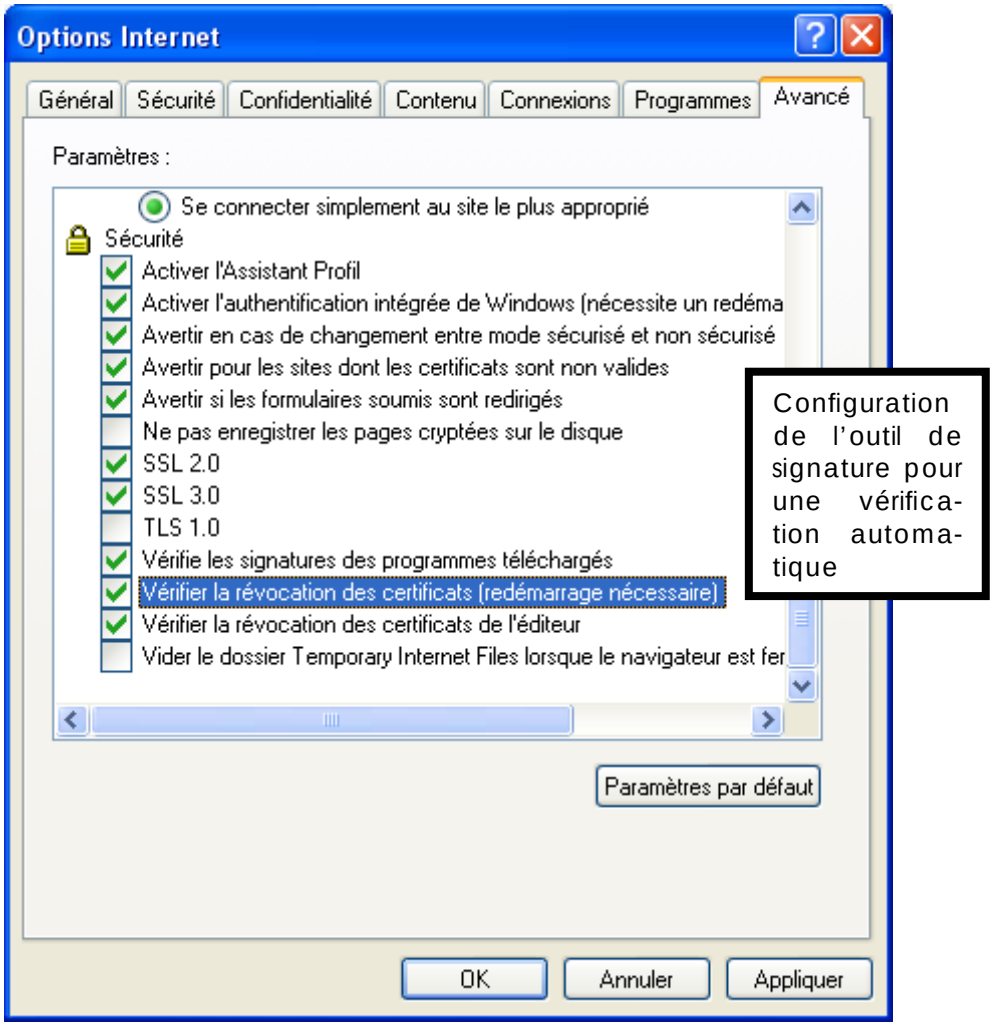
- du porteur du certificat (eg : en cas de perte du code secret –PIN-) ;
- de l'autorité de certification (eg : en cas de non paiement du certificat par le porteur) ;
- de l'organisation qui a acheté un certificat pour l'un de ses membres lors du départ de celui-ci.

La révocation peut intervenir à tout moment et il faut donc vérifier le certificat à chaque utilisation.

L'utilisateur peut télécharger la liste des certificats révoqués publiée par l'AC émettrice du certificat :



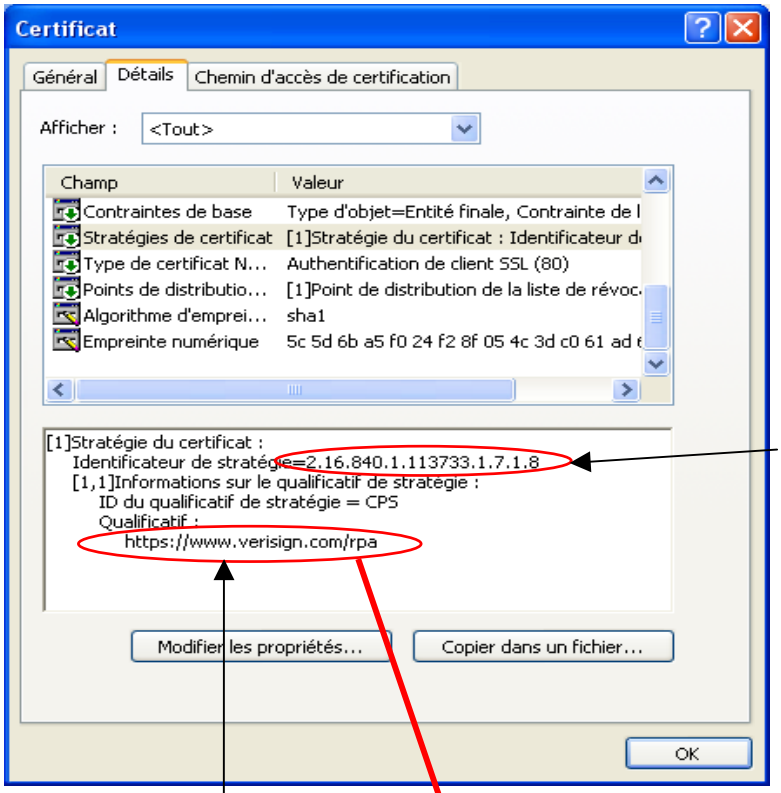
…ou demander à l'outil de signature de le vérifier automatiquement :



Bien sur, pour cela il faudra être connecté…

Les autorités de certification sont très vigilantes sur le point de savoir si les conditions d'usage des certificats sont bien respectées.

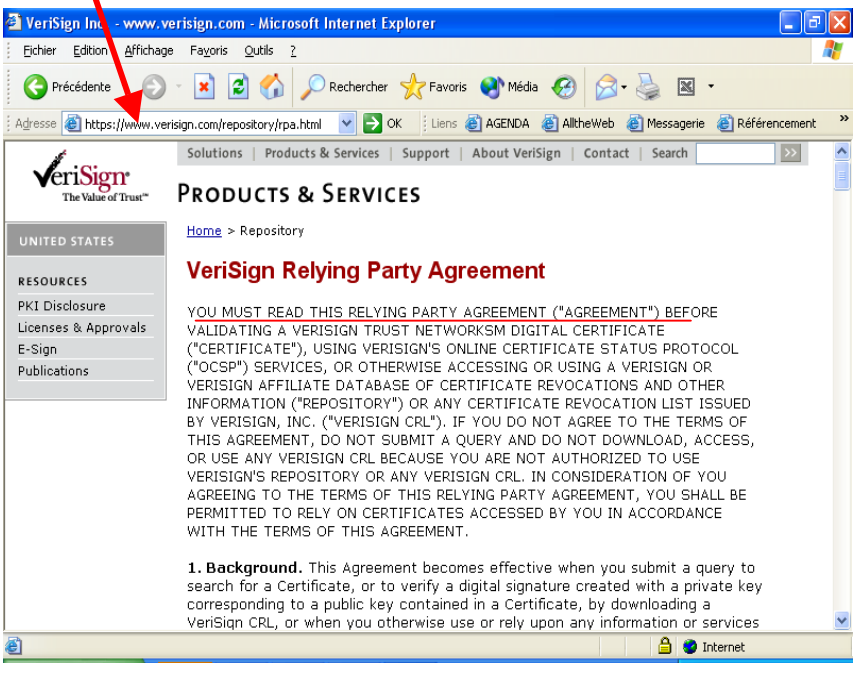
Celles-ci font toujours l'objet d'une publication sur le site de ces organisations. Ces conditions sont appelées *Politiques de certification* et elles sont identifiées. Ce numéro unique et l'adresse de publication peuvent être rappelés dans le certificat lui-même.



Avant d'utiliser de façon habituelle un certificat il est vivement recommandé de lire ce document afin d'en avoir un usage ad hoc et de bénéficier de la garantie de l'AC.

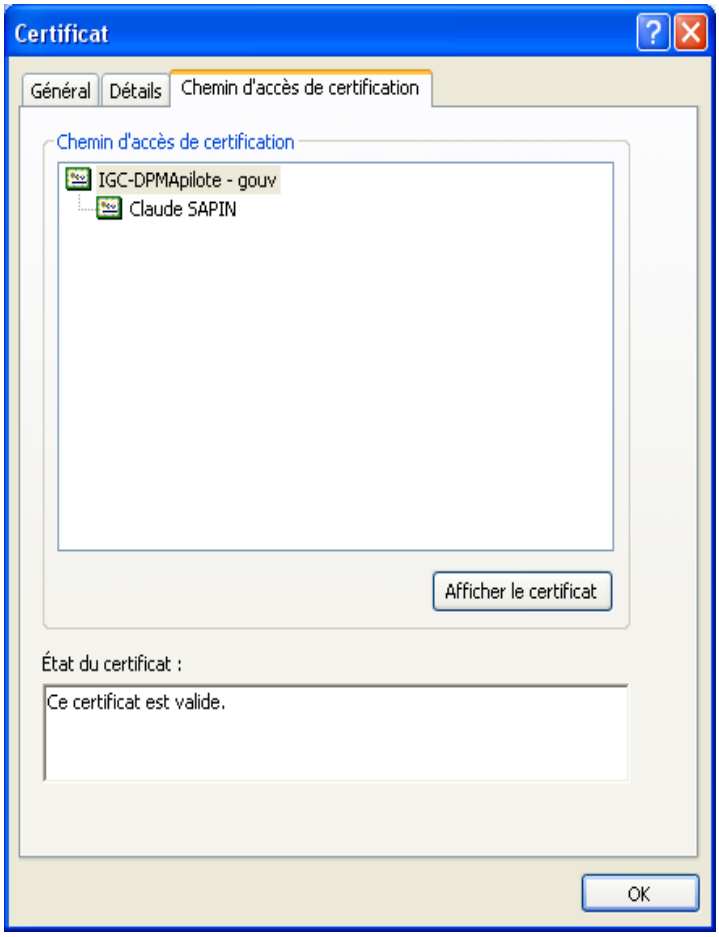
OID du document (numéro unique attribué par un organisme normalisateur. Sur l'internet l'ISO ou IANA.)

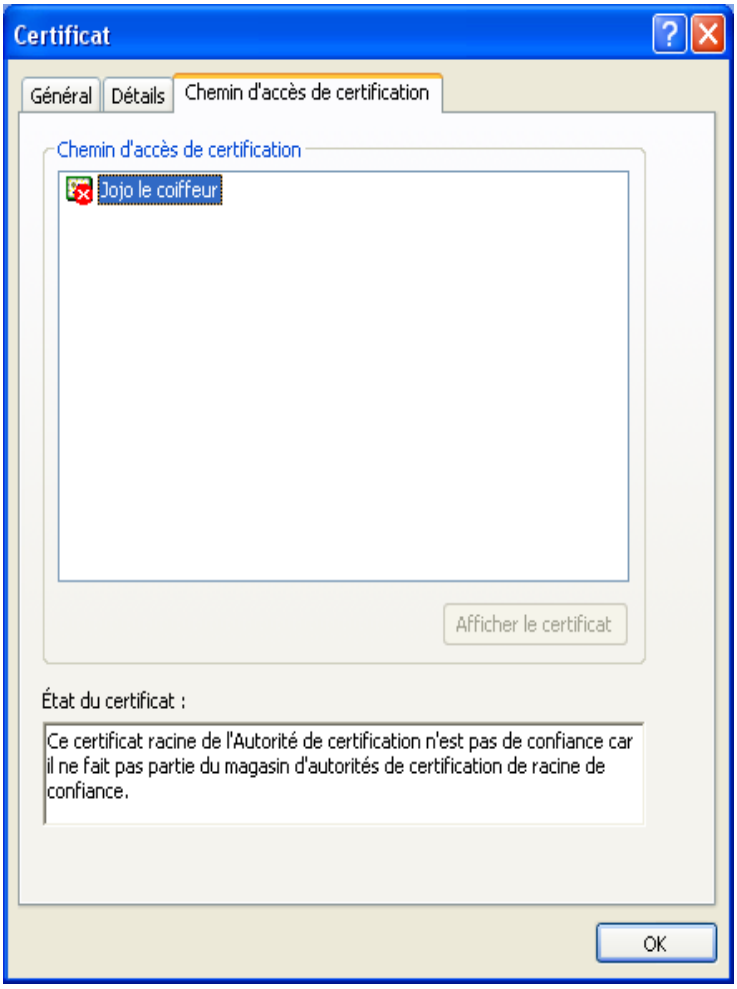
L'adresse (URL) où est publié le document



4. Comment faire confiance au certificat ?

En réalité c'est à l'**autorité de certification** (AC) qui a émis le certificat que l'on fait confiance.





Il est possible que l'une de ces deux AC inspire plus de confiance que l'autre ?

Une autorité de certification[14] est une entreprise qui garantit :

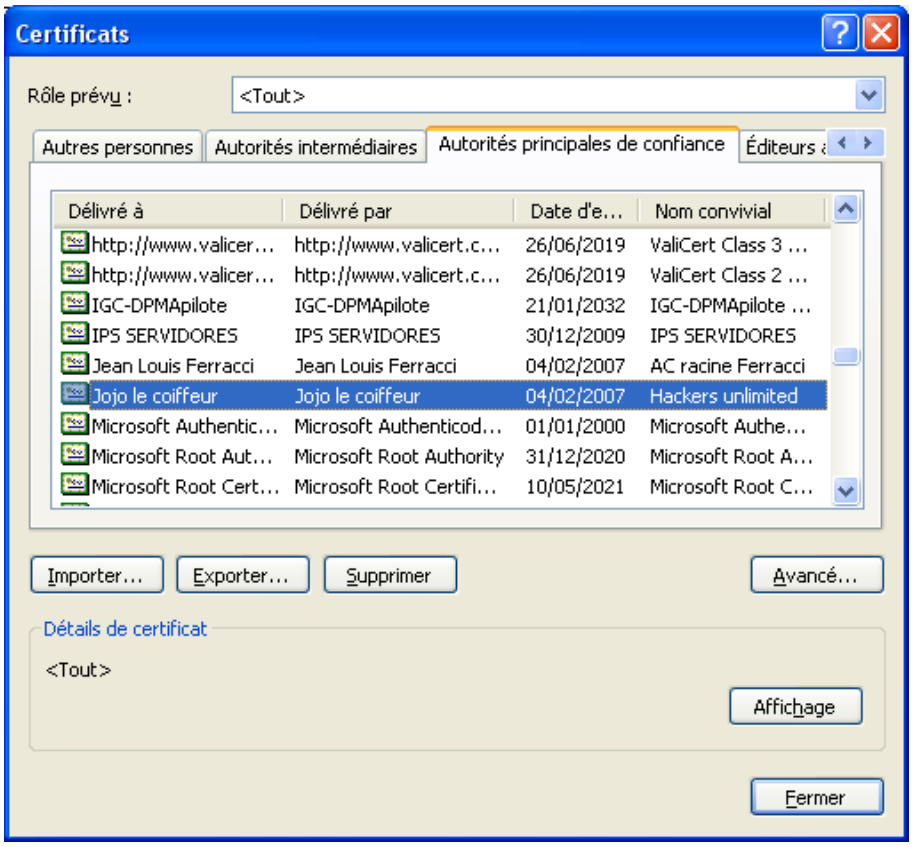
- l'identité de la personne qui utilise des clés de signature. Cette garantie peut être plus ou moins grande selon le protocole utilisé (et donc le coût). Les certificats utilisés par les téléprocédures du MINEFI sont tous délivrés en face à face avec une production de papiers d'identité ;
- L'usage des clés par une personne qui en est la seule et unique propriétaire.

Le certificat concrétise cette garantie.

[14] La terminologie utilisée dans ce secteur est souvent directement traduite de l'anglais (américain) ce qui peut lui donner une emphase inappropriée.

5. Comment faire confiance à une autorité de certification ?

Chacun le sait, la confiance ne doit être accordée que parcimonieusement et après investigations. Il ne suffit pas en effet d'apparaître dans la liste des autorités principales de confiance de son outil de signature pour être une AC sérieuse apte à délivrer des certificats convenablement : Jojo le coiffeur s'est aussi immiscé dans la liste des autorités principales de confiance !



Mais alors à qui faire confiance si même ce qui apparaît dans le navigateur est sujet à caution?

Trois moyens sont offerts :

5.1 Les institutions publiques publient des listes de certificats acceptables émis par des entreprises dont la réputation, le modèle économique et les processus techniques ont fait l'objet d'un audit, ce qui leur permet d'être référencé selon des critères de qualité élevés.

C'est ce que fait le MINEFI et l'ADAE prendra le relais bientôt :
http://www.minefi.gouv.fr/dematerialisation_icp/dematerialisation_declar.htm

Ceux-ci sont décrits dans la *politique de certification type* du MINEFI (même URL que ci-dessus) et dorénavant dans la *politique de référencement intersectoriel de sécurité* (PRIS) qui est disponible sur le site de l'ADAE.

Ces certificats sont acceptés pour toutes les téléprocédures de la sphère publique conformément aux prescriptions de l'ADAE. Il est possible de vérifier que Jojo le coiffeur n'y figure pas et donc d'être assuré que les envois signés et accompagnés par un certificat référencé offre toutes les garanties requises pour des échanges hautement sécurisés.

5.2 Les éditeurs d'outils de signature intègrent les certificats racines des AC

Les éditeurs d'outils de signature (Lucent technology, Microsoft, Sun, etc.) intègrent dans les magasins de certificats, et dès la production, les certificats racines des AC qu'ils ont agréés selon un processus qui leur est propre. Il est bon de s'assurer que ceux qui y figurent sont bien ceux que l'éditeur a choisi d'y mettre en comparant la liste fournie par le navigateur et celle publiée sur leurs sites.

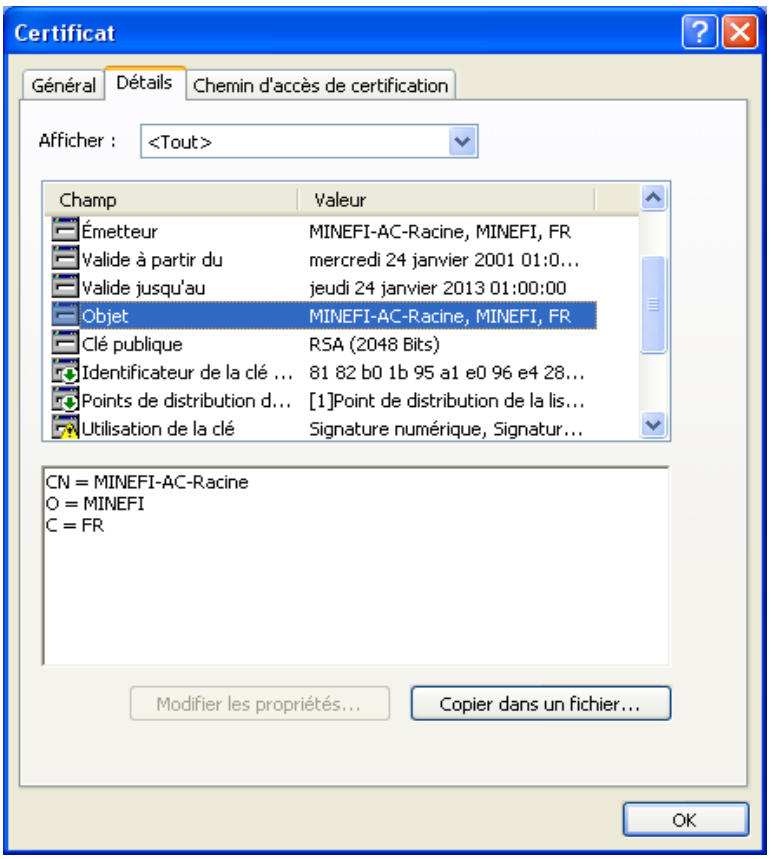
Il n'est pas inutile non plus de se souvenir que les prescriptions en matière de sécurité demandent une acceptation consciente des certificats. La bonne pratique consistant donc à ôter tous les certificats pour n'intégrer qu'au fur et à mesure ceux dont le besoin et la qualité justifient l'usage.

5.3 Il est possible de faire confiance à une AC dont on connaît les promoteurs

En effet bien que ne figurant ni dans la liste publiée par le MINEFI, ni dans celles des éditeurs (en général car elles n'appartiennent pas au secteur marchand) elle sont tout à fait respectables.

Le MINEFI par exemple, mais le CNRS, le ministère de la Justice, de l'Education nationale, et bien d'autres. organisations sont dans ce cas.

En résumé il y a donc les autorités de certification « conseillées », dont certains certificats sont référencés par l'Etat, voire par les éditeurs, et celles auxquelles il est fait confiance par un choix personnel et éclairé.



Ces certificats sont fiables, les règles d'usage sont connues et leurs titulaires identifiés pourront être retrouvés si nécessaire.

La confiance est établie.

ANNEXE 3 : les certificats de chiffrement dans le cadre de la dématérialisation des achats

1. Contexte et enjeu :

En général, la confidentialité est obtenue en chiffrant avec la clé publique publiée par la plate-forme (ou tout autre moyen) qui publie l'appel d'offre auquel il est répondu[15]. L'enjeu est celui de la disponibilité, juste à temps, de la clé privée (clé de déchiffrement) qui, en attendant l'ouverture des plis, a du rester secrète.[16]

2. Les étapes de l'échange

2.1 Publication

Une personne responsable des marchés (PRM) transmet à une plate-forme les appels d'offres qu'elle souhaite publier. La plate-forme (PF) publie les appels d'offres et publie simultanément la clé publique du certificat de chiffrement qui devra être utilisée pour chiffrer les réponses à cet appel d'offres.

2.2 Réponses des entreprises

a) <u>à la plate forme</u> :

La PF chiffre elle-même les fichiers qui sont présentés par l'entreprise pour garantir la confidentialité des réponses qu'elle reçoit et stocke en attendant le jour de l'ouverture des plis. Dans ce cas il est impératif que la transmission soit chiffré par un autre moyen (canal SSL) et que le processus de chiffrement sur la plate-forme soit de grande confiance, pour garantir que l'offre qu'elle recevra donc en clair ne sera pas divulguée avant qu'elle ait pu être chiffrée.

Le chiffrement peut aussi être réalisé par l'entreprise, sans intervention de la plate-forme pour garantir la confidentialité des réponses qu'elle envoie et qui seront stockées en attendant le jour de l'ouverture des plis.

b) <u>par un autre canal que la plate-forme</u> :

Le chiffrement est réalisé par l'entreprise elle-même pour garantir la confidentialité des réponses qu'elle envoie et qui seront stockées en attendant le jour de l'ouverture des plis.

2.3 Ouverture des plis :

Les plis ont été réceptionnés par une plate-forme qui fournit aussi les clés de chiffrement :

- Celle-ci communique à la PRM sous pli scellé (postal, porteur ou courriel) la clé privée de chiffrement ;
- La mise au clair se fait uniquement sur le poste de la PRM.

Les plis n'ont pas été réceptionnés par l'organisation qui fournit les clés de chiffrement :

[15] D'autres façons de chiffrer sont envisageables, notamment celles qui nécessitent la collaboration de l'entreprise pour le déchiffrement ; elles sont moins commodes d'emploi et ne sont donc pas abordées ici.

[16] *Rappel* : on chiffre avec la clé *publique* du destinataire ce que l'émetteur (ici l'entreprise) veut lui envoyer de façon confidentielle. Le destinataire (ici la PRM) déchiffre avec sa clé *privée*.

- La clé privée de chiffrement est conservée par un autre service que celui de la PRM : elle doit recevoir sous pli scellé (postal, porteur ou courriel) la clé privée de chiffrement ;
- La PRM dispose déjà de la clé privée (génération locale du bi-clé de chiffrement, par exemple sur une carte à puce) :
  - Elle doit s'assurer que la procédure d'usage de la clé privée (code PIN, support de la clé privée, etc.) est disponible et que ce qu'elle prévoit est réalisable ;
  - Toutes les précautions d'organisation doivent être prises pour que la PRM ne puisse pas prendre connaissance des offres avant la CAO.
- Dans tous les cas **la mise au clair se fait exclusivement sur le poste de la CAO**.

3. Pour améliorer l'usage du certificat de chiffrement

3.1 Observations sur certains facteurs de risques

- Si une plate-forme fournit aussi les clés de chiffrement il existe un séquestre de fait de la clé privée et pour cette raison sa responsabilité pourra toujours être engagée ;
- Une forte séparation entre les fonctions de séquestre et celles de PF est donc indispensable. Elle doit être garantie dans le marché qui doit prévoir en outre qu'elle puisse être auditable afin de permettre le cas échéant un examen ultérieur[17] ;
- Le respect des conditions attendues de délai et de sécurité de réception de la clé privée est indispensable à la bonne marche de l'opération, car sans lui pas d'ouverture des plis possible, voire même une ouverture contestable.

3.2 Mesures d'organisation suggérées

Il peut être utile pour la PRM de définir au moins trois procédures :

- Non réception du pli contenant la clé privée et mesures de sécurité à prendre :
  - que faire lors de la séance si le pli n'est pas arrivé ?
  - que faire du pli qui arrivera après le nouvel envoi par la plate forme : destruction avec procès verbal, conservation avec le nouveau, etc.?
  - que faire en cas de perte du pli car les offres, même conservées chiffrées, deviendront alors potentiellement lisibles par le détenteur illicite ?
- Réception de la clé privée et conservation dans des conditions adaptées de sécurité (armoire forte, coffre, etc.), en séparant selon le cas le support (carte à puce ou clé USB) du code PIN (« personal identity number ») ;
- Protection des agents de la PRM contre des soupçons possibles en publiant publiquement les procédures écrites, et en mettant effectivement à disposition les moyens techniques qui y sont décrits.

3.3 Précautions éventuelles

- Le certificat de chiffrement devrait être fourni à une entité et non à une personne. Le code PIN d'activation devrait être tenu secret sous pli confidentiel jusqu'à la date d'ouverture, sa remise à la personne ad hoc s'accompagnant d'une mention au procès-verbal de la séance. En effet la remise d'un code PIN à une seule personne possible, car nommément désignée dans la procédure de délivrance, et qui pourrait être absente, fait courir un risque d'échec élevé à la procédure ;
- Les PRM devraient encourager à terme la procédure dite « des quatre yeux » qui améliore notablement la sécurité. (Deux personnes ont chacune un certificat différent).

[17] L'auditabilité d'un système est la propriété qui assure la capacité à détecter et à enregistrer de façon infalsifiable les tentatives de violation de la Politique de sécurité.

ANNEXE 4 : l'authentification des personnes et des serveurs

1. Définitions : authentification et identification

1.1 Identification

C'est le fait pour une personne de **décliner son identité**. L'identification par la plate-forme ne comporte aucun contrôle, elle est purement déclarative car elle a été réalisée en face à face lors de la délivrance du certificat.

1.2 Authentification

C'est le fait pour une personne de **prouver que l'identité.qu'elle revendique est bien la sienne**. Cela peut se faire par la présentation d'un mot de passe connu uniquement de son porteur légitime ou par l'utilisation d'une clé privée dans le cadre de l'authentification par certificat.

2. Authentification des serveurs

Pour les connexions web sécurisées en https (SSL/TLS), le serveur s'authentifie auprès de la personne qui y accède. Cette authentification ne se matérialise pour l'utilisateur que par le préfixe https présent en tête de l'adresse du serveur et par l'apparition du cadenas fermé sur le navigateur.

Il s'agit d'une authentification par certificat : le navigateur vérifie que l'adresse indiquée dans le certificat du serveur est bien celle à laquelle l'utilisateur est connecté.

Si le certificat du serveur a été émis par une Autorité de certification non reconnue par le navigateur de l'utilisateur, une fenêtre d'avertissement est présentée, et l'utilisateur doit décider s'il accorde ou non sa confiance au site auquel il est en train d'accéder. Les certificats de certains grands prestataires de services de certification (PSC), généralement américains, comme Verisign ou Thawte par exemple sont reconnus d'origine par les navigateurs, ce qui ne signifie pas pour autant que d'autres certificats, émis par d'autres prestataires de certification, soient moins dignes de confiance. Lorsque son navigateur ne reconnaît pas automatiquement un certificat, l'utilisateur doit donc examiner s'il a bien été émis par un prestataire de services de certification à qui il estime pouvoir faire confiance. Ces opérations sont à faire la première fois que l'utilisateur rencontre un certificat émis par un PSC qui n'a pas déjà été intégré dans le magasin à certificats de son navigateur, mais elle doit être faite avec soin. En effet accepter un certificat entraîne automatiquement que le PSC sera dorénavant automatiquement reconnu par le navigateur.

Lorsque l'on accède à un serveur ainsi sécurisé, on peut avoir raisonnablement confiance dans le contenu que l'on télécharge.

Pour l'accès à une plate-forme de dématérialisation, et pour éviter le risque qu'il s'agisse d'un faux site, l'utilisateur doit également vérifier que le certificat que présente le serveur est bien celui qu'a publié la plate-forme à qui il pense s'adresser (cf. § 5.1 du guide, mesures à prendre par la plate-forme « le certificat de la plate-forme doit être publié de façon fiable et commodément accessible, par exemple dans la presse ; la plate-forme doit indiquer sur quel support il est possible de vérifier son certificat »).

3. Authentification pour contrôle d'accès

Les utilisateurs qui doivent accéder à des serveurs ou à des services à accès contrôlé sur Internet doivent s'identifier (déclarer qui ils sont) et s'authentifier (prouver qui ils sont) de manière à permettre au serveur ou au service de vérifier qu'ils sont bien habilités à y accéder.

La gestion des habilitations (ou gestion des droits) est un sujet à part entière, qui vient en aval de l'authentification, et n'est pas traitée dans la présente fiche.

Quelle authentification ? Il existe plusieurs modes d'authentification, qui présentent des caractéristiques différentes en termes de facilité et de coût de déploiement, de simplicité d'utilisation, de sécurité offerte. Le présent paragraphe compare les authentifications par mot de passe et par certificat (parfois appelée, à tort, « authentification forte »).

3.1 Authentification par identifiant / mot de passe

Description : Dans un formulaire, l'utilisateur saisit son identifiant et un mot de passe qui doit demeurer connu de lui seul. Dans la plupart des systèmes, ce mot de passe peut être changé par l'utilisateur, qui peut ainsi le choisir facile à mémoriser.

Coût de déploiement : Le coût est très faible et ce type d'authentification est extrêmement répandu.

Simplicité d'utilisation : La simplicité est extrême. Une telle authentification peut être employée depuis tout poste de travail.

Attaques :

- Attaque de proximité : les utilisateurs ont tendance à inscrire leur mot de passe sur un support autocollant à côté de l'ordinateur.
- Un pirate écoutant la ligne peut prendre connaissance du message qui transite et le rejouer pour se faire passer pour le porteur légitime.
- Attaques par dictionnaire : essayer de nombreux mots de passe en espérant tomber sur le bon ; il suffit de quelques secondes pour deviner ainsi un mot de passe de quelques caractères ; le temps nécessaire croît exponentiellement avec le nombre de caractères.

Parades : Pour l'utilisateur, employer des mots de passe simples à retenir, de préférence au choix de l'utilisateur, pour éviter de le retrouver écrit partout, tout en veillant à ce qu'ils ne soient pas facile à deviner (mélange de caractères alphabétiques, numériques et de ponctuation, longueur supérieure à 7 caractères etc.) ; les conserver en lieu sûr, aussi bien pour les retrouver en cas d'oubli que pour que des personnes non autorisées ne les utilisent indûment.

Pour les concepteurs des systèmes, effectuer la présentation du mot de passe dans une session sécurisée https (très facile à mettre en œuvre, très efficace) et limiter le nombre de présentations successives possibles (très facile à mettre en œuvre. Ouvre la possibilité de déni de service ciblé en bloquant le compte de quelqu'un). Autre solution : la détection des attaques par dictionnaire peut se faire au niveau pare-feu (moyennement complexe à mettre en œuvre, efficace).

Entité identifiée : Ce mode d'authentification permet de s'assurer que la personne utilisant le service est bien en possession du mot de passe.

Niveau de sécurité : Employé dans de bonnes conditions (mot de passe facile à retenir, présenté dans une session sécurisée, avec un système empêchant les attaques par dictionnaire), le « login » / mot de passe offre une bonne sécurité, c'est-à-dire une bonne garantie de l'identité de l'utilisateur qui se connecte.

3.2 Authentification par certificat sur support physique

Description : l'utilisateur dispose d'une carte à puce ou d'une clé USB contenant son certificat. Lors de l'authentification, on lui demande d'introduire ce support physique et de saisir son code porteur (généralement à 4 chiffres).

Coût de déploiement : le coût est plus élevé car il comprend d'une part le matériel, d'autre part la mise à niveau des postes de travail, et surtout une organisation complexe pour gérer les certificats (révocation, expiration, gestion des oublis, formation et sensibilisation du personnel).

Simplicité d'utilisation : Par analogie avec la carte bleue, l'utilisation est relativement simple. Une telle authentification ne peut être employée que depuis un poste de travail muni d'un logiciel adéquat, ce qui limite son champ d'utilisation.

Attaques : attaque de proximité : les utilisateurs ont tendance à laisser leur carte ou clé USB à côté de l'ordinateur, voire dans le lecteur.

Parades : l'utilisateur peut choisir son code porteur, ce qui évitera qu'il l'inscrive sur sa carte ! La sensibilisation du personnel est facilitée par l'analogie avec la carte bleue.

Entité identifiée : ce mode d'authentification permet de s'assurer que la personne utilisant le service est bien en possession du support physique et connaît le code porteur. La clé privée contenue sur le support physique ne peut pas être dupliquée. De plus, une telle authentification, même espionnée, n'est pas rejouable. C'est en cela que l'on parle d'« authentification forte ».

Niveau de sécurité : l'authentification par certificat sur support physique offre le meilleur niveau de sécurité.

3.3 Authentification par certificat logiciel

Description : l'utilisateur dispose d'un certificat logiciel stocké sur son poste de travail : il y a donc sur ce poste un objet informatique sensible, contrairement aux deux solutions examinées précédemment. Lors de l'authentification, selon la configuration de son poste, l'utilisateur doit choisir dans une liste le certificat destiné à l'authentifier et/ou saisir un mot de passe de déblocage.

Coût de déploiement : le coût est assez élevé car il comprend le coût des certificats, et surtout, comme pour les certificats sur support physique, une organisation complexe pour les gérer (révocation, expiration, changement de poste, formation et sensibilisation du personnel).

Simplicité d'utilisation : l'utilisation est relativement simple, comme pour les certificats sur support physique.

Attaques : les attaques particulières à ce mode d'authentification ont pour but principalement d'accéder au certificat stocké sur le poste de travail :

- Attaque de proximité : le certificat étant installé sur le poste, il suffit d'accéder à la machine pour se faire passer pour le porteur légitime du certificat ; le poste doit donc être sécurisé contre les accès physiques illicites : parmi les mesures à envisager, il faut penser d'abord au contrôle d'accès aux locaux pour que seules des personnes de confiance puissent y pénétrer, à mettre au minimum un mot de passe pour le démarrage de la machine et son écran de veille, à ne pas laisser la machine en fonction sans surveillance, voire à interdire son démarrage par l'utilisateur sur un autre support (disquette, CD-ROM) que son disque dur,
- Attaque à distance : pour la même raison, toute attaque à distance sur le poste peut compromette le certificat : le réseau auquel est connecté le poste doit être sécurisé, contre les attaques externes (pare-feu au raccordement à internet, antivirus, anti-espiogiciel et correctifs des progiciels à jour etc.) et contre les attaques internes (pare-feu individuel) si elles ne sont pas écartées.
- Duplication : le certificat logiciel peut être copié, contrairement au cas des supports physiques.

Parades :

- Protéger l'utilisation du certificat par la présentation systématique d'un mot de passe (tâche d'administration du poste assez complexe, risque d'oubli des mots de passe) ;
- Interdire l'export de la clé privée (tâche d'administration lors du déploiement ou quand l'utilisateur change de poste de travail).

Entité identifiée : ce mode d'authentification permet d'authentifier le poste de travail de l'utilisateur. L'authentification par certificat logiciel bénéficie parfois à tort de l'appellation « authentification forte » alors qu'elle est bien plus faible que si l'on dispose d'un support physique et en rien meilleure que le mot de passe.

Niveau de sécurité : l'authentification par certificat logiciel offre une apparence de sécurité du fait de la réputation des certificats, mais si le poste de travail où il est stocké n'est pas sécurisé, ce n'est qu'un leurre dont le danger mérite d'être mis en lumière.

ANNEXE 5 : gestion des virus dans le cadre de la dématérialisation des achats

1.Cadre réglementaire

Décret n° 2002-692 du 30 avril 2002 – Article 10 : tout document électronique envoyé par un candidat dans lequel un virus informatique est détecté par l'acheteur public peut faire l'objet par ce dernier d'un archivage de sécurité sans lecture dudit document. Ce document est dès lors réputé n'avoir jamais été reçu et le candidat en est informé.

Ce cadre est complété par les indications du vade-mecum juridique sur la dématérialisation des marchés publics, qui seront citées lorsque cela sera justifié.

2. Emplacement de l'anti-virus

La dématérialisation amenant les collectivités et les entreprises à échanger des fichiers, il est nécessaire que chacun se protège et protège l'autre de toute infection par une inspection systématique des éléments transmis.

En règle générale, tout réseau d'entreprise ou de collectivité inclut un antivirus déployé sur les postes de travail. Toutefois, il est très fréquent que ces antivirus ne soient pas à jour, soit que la procédure soit manuelle, soit qu'elle soit automatique mais incorrectement configurée, soit même qu'elle ne soit pas définie.

On doit donc mettre en place deux modes d'inspection des fichiers contre les virus, qui sont complémentaires : l'emploi d'un anti-virus mis en commun sur la plate-forme de dématérialisation pour les fichiers non chiffrés, et l'emploi d'un anti-virus local sur le poste de travail.

3. Antivirus de plate-forme

Un service antivirus proposé par la plate-forme de dématérialisation (ou le service de dématérialisation s'il est internalisé) ne nécessite aucune installation sur le poste de l'utilisateur du service, puisqu'il s'agit d'un service rendu en ligne sur les fichiers envoyés sur la plate-forme, et non d'une inspection du poste de travail de l'utilisateur.

La mise en commun d'un antivirus sur le serveur pour l'ensemble des utilisateurs de la plate-forme permet à chacun (entreprises comme collectivités publiques) de disposer en permanence d'un service d'antivirus à jour pour les documents qu'elle transmet à la plate-forme ; cela ne la dispense pas d'effectuer des actualisations de son parc informatique.

Les signatures de virus sont en général mises à disposition quotidiennement par les éditeurs d'antivirus, ce qui permet de tenir à jour de manière très sécurisée le service de protection.

En revanche, un tel service ne pourra pas inspecter les plis chiffrés, comme l'explique le vade-mecum :

Vade-mecum, §9.4 : Sachant notamment qu'un dossier chiffré ne peut pas faire l'objet d'une détection antivirale, il a ainsi pu être imaginé qu'un dossier chiffré soit déchiffré à sa réception, passé à l'anti-virus, puis si ce contrôle est négatif, chiffré à nouveau avant d'être placé dans un coffre-fort électronique avant son ouverture. […]
Après analyse, il apparaît qu'une telle pratique ne respecterait pas la confidentialité des candidatures et des offres jusqu'à leur ouverture. En effet, il faut savoir qu'à partir du moment où un document chiffré est déchiffré, il peut être lu et rien ne permet de rapporter la preuve que celui qui l'a déchiffré ne l'a pas lu.

Cette approche n'est d'ailleurs pas différente de celle qu'adopte la directive 2004/18/CE du Parlement et du Conseil du 31 mars 2004.

4. Antivirus local

Il faut de toutes façons recourir de plus à un anti-virus installé localement sur le poste de travail et le tenir à jour quotidiennement ; on aura soin de ne pas ouvrir un fichier avant de l'avoir inspecté.

L'anti-virus du poste peut être configuré pour inspecter automatiquement tous les fichiers au moment de leur écriture sur le disque, ce qui est le mécanisme le plus simple. L'inspection peut également être réalisée manuellement.

5. Détection des virus dans les dossiers d'appel à candidature et les DCE

Afin de protéger les entreprises contre d'éventuelles infections provenant de la collectivité publique, il est nécessaire que lors du dépôt par la collectivité publique de son dossier d'appel à candidatures ou de son DCE, les fichiers constituant ce dossier soient inspectés par l'antivirus, d'abord sur le poste de travail qui les transmet à la plate-forme et ensuite par l'antivirus de la plate-forme.

Si un virus est détecté par la plate-forme, le dossier complet est supprimé de la plate-forme, et en retour la collectivité publique en est informée, par un message (mail ou affiché à l'écran) indiquant le nom des fichiers infectés et le nom des virus découverts.

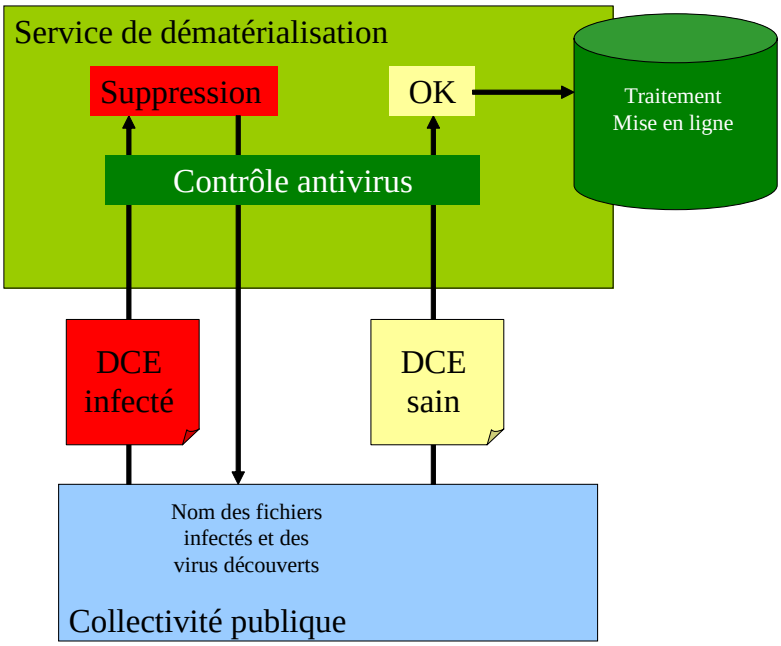


Figure 1 : Fonction antivirus pour les DCE

6. Détection des virus dans les échanges

L'envoi par la collectivité publique ou par une entreprise d'un courrier électronique dans le cadre de la dématérialisation peut se faire de plusieurs manières : un service classique de messagerie peut être employé, mais sa sécurité étant insuffisante (cf. annexe 14), il est alors nécessaire de prendre des précautions particulières pour lui assurer le niveau de sécurité nécessaire (cf. annexe 14) ; on peut aussi recourir à un service particulier de courriers électroniques recommandés avec accusés de réception.

Dans le cas de l'utilisation de la messagerie classique, c'est l'antivirus classique de la messagerie qui sera employé.

Dans le cas d'un service de messagerie recommandée avec accusés de réception, en général, les pièces jointes et le texte du mail seront disponibles sur la plate-forme de courrier recommandé (certains prestataires de services de dématérialisation proposent ce service sur la même plate(forme que celle qui est utilisée pour mettre en ligne l'AAPC et le DCE, et recevoir les candidatures et les offres) dans un sas d'échanges sécurisé après réception par le destinataire d'un bordereau de mise à disposition transmis par simple mail. Les fichiers joints stockés par la plate-forme pourront alors être inspectés sur la plate-forme par l'antivirus.

Si un virus est détecté, le courrier complet est supprimé de la plate-forme, et en retour l'émetteur en est informé, par un message indiquant le nom des fichiers infectés et le nom des virus découverts.

Si aucun virus n'est détecté, le courrier est stocké dans le sas d'échanges sécurisé et mis à disposition du destinataire.

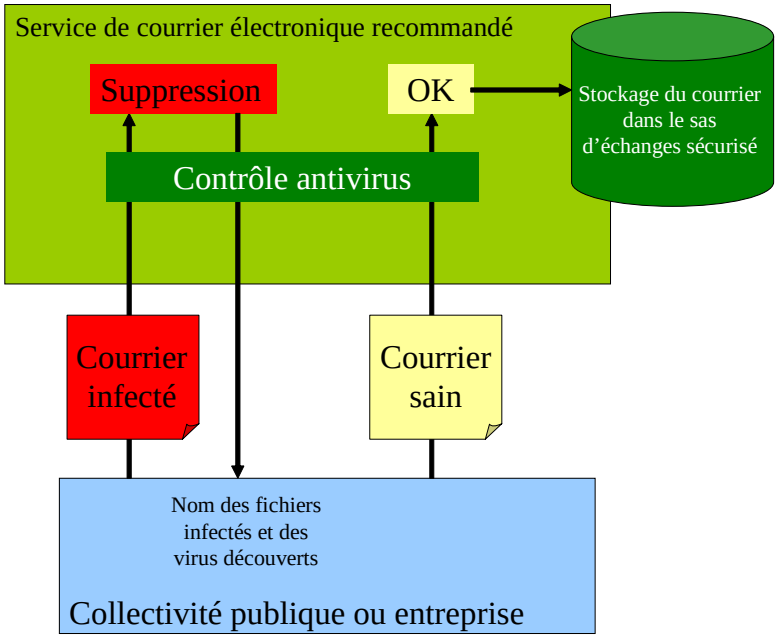


Figure 2 : Fonction antivirus pour le sas d'échanges sécurisé

7. Détection des virus dans les plis des soumissionnaires

Dans l'absolu, la détection antivirus concernant les plis des soumissionnaires peut être réalisée à trois moments distincts :

7.1 Détection des virus avant le dépôt du pli par le soumissionnaire

Les plis chiffrés ne pouvant pas être inspectés par l'anti-virus de la plate-forme de dématérialisation, les entreprises qui déposent un pli doivent inspecter leurs fichiers contre les virus sur leur poste local, avec un anti-virus à jour, **avant** de chiffrer le pli et de le faire parvenir à la collectivité publique.

Cette précaution réduit les risques de rejet pour cause de présence de virus sans toutefois complètement les annuler, puisqu'il est possible qu'un virus soit présent dans un fichier au moment de l'inspection, mais non encore connu des éditeurs d'anti-virus. Si un tel virus est mis au jour entre le moment du dépôt du pli et le moment de son inspection par la collectivité publique, l'entreprise aura de bonne foi déposé un pli qu'elle pensait inoffensif, alors qu'un virus y aura été détecté.

La plate-forme de dématérialisation ne doit pas prendre la responsabilité d'une inspection préalable, car d'une part elle prendrait ainsi connaissance des offres et d'autre part aucun engagement ne peut être pris sur la validité d'une telle inspection du fait du laps de temps qui la sépare de l'ouverture du pli. Pour les mêmes raisons (divulgation de sa proposition, délai entre le dépôt de l'offre et la CAO d'ouverture des plis), l'entreprise ne doit pas recourir aux services de détection de virus en ligne que proposent les éditeurs d'antivirus.

7.2 Détection des virus lors du dépôt du pli

La détection de virus dans un pli nécessite de disposer du pli en clair et de pouvoir accéder à son contenu. Or le principe de confidentialité des offres interdit à une plate-forme de dématérialisation de connaître le contenu des plis.
On garantit la confidentialité des plis de bout en bout en réalisant un chiffrement des plis sur le poste du soumissionnaire et en n'effectuant le déchiffrement qu'au moment de la CAO lorsque la collectivité publique a décidé d'ouvrir le pli.
Or la détection de virus sur un pli chiffré n'est pas possible.

7.3 Détection des virus lors de l'ouverture des plis par la collectivité publique

C'est en CAO, lorsqu'elle décide d'ouvrir les plis, que la collectivité publique doit réaliser un contrôle antivirus des fichiers reçus. Elle doit donc disposer d'un antivirus à jour sur le poste de CAO, antivirus qui s'exécute alors lors du déchiffrement des plis et inspecte les fichiers clairs ainsi créés avant leur ouverture pour examen. Il est indispensable de prendre alors les précautions qui donneront les assurances nécessaires et assureront la traçabilité des opérations (cf. annexe 6) : nettoyage préalable, avec un antivirus à jour, de la machine où sont ouvertes les offres, garanties qu'une offre qui serait porteuse de virus ne contamine pas les autres etc.

Certaines plates-formes proposent un service permettant, au moment de l'ouverture des plis, une fois les clés téléchargées par la collectivité, de réaliser un premier déchiffrement et une inspection sur la plate-forme de dématérialisation avant d'effectuer le déchiffrement sur le poste de la collectivité.
Un tel service permet de protéger le poste de la CAO contre les virus et assure une mise en quarantaine automatique ; il est clair cependant qu'il, rompt la chaîne de la confidentialité (cf. vademecum juridique § 9.4) puisqu'il donne accès aux offres à la plate-forme de dématérialisation, alors que seules la PRM, la CAO et l'entreprise soumissionnaire doivent pouvoir y accéder. Bien que cette opération n'intervienne qu'une fois la décision d'ouverture des offres prises par la CAO, la personne publique ne doit recourir à ce service optionnel qu'avec prudence, en s'assurant que l'enjeu de la consultation le permet et que les conditions dans lesquelles la plate-forme prend ainsi connaissance des offres garantissent bien la sécurité nécessaire.

8. L'archivage de sécurité

> **Vade-mecum, § 10.4 :** […] l'acheteur public « peut » décider que le document contaminé par un virus fera l'objet d'un archivage de sécurité, et a contrario, il peut décider que ce document ne fera pas l'objet d'un tel archivage.
> Dans le premier cas, la sanction de l'archivage de sécurité est claire : le document contaminé est réputé n'avoir jamais été reçu.
> Dans le second cas, l'intérêt de l'acheteur est de mettre en œuvre un programme de réparation du document contaminé.
> […]
> Dans le cas où un archivage de sécurité est décidé, le système mis en œuvre devra garantir que le document ne sera pas ouvert.

Dans le cas où la collectivité publique détecte la présence d'un virus dans un pli, elle a la possibilité de mettre le pli correspondant en quarantaine, dans ses locaux.

La mise en quarantaine doit :

- assurer que le document ne sera pas ouvert ultérieurement par inadvertance (afin d'éviter la contamination) ou par curiosité (puisqu'il est réputé n'avoir jamais été reçu) ;
- permettre de l'exhiber ultérieurement en cas de contentieux afin de pouvoir prouver qu'il a bien été rejeté avec raison : il convient donc que l'anti-virus fournisse une liste précise des fichiers infectés et des virus découverts dans ces fichiers, et que cette liste accompagne les fichiers mis en quarantaine.

Si les fichiers contaminés sont mis en quarantaine en clair, des précautions doivent donc être prises pour en restreindre l'accès aux cas de contentieux, en évitant toute erreur qui propagerait les virus dont ils sont porteurs, et toute curiosité déplacée. Si les fichiers sont mis en quarantaine chiffrés, les clés de déchiffrement doivent être conservées, et protégées pour n'être mises en œuvre qu'en cas de contentieux.

Il est nécessaire de coupler le service de quarantaine avec une suppression des fichiers sur le poste où ils avaient été préalablement déchiffrés et où le contrôle anti-virus avait été effectué, ne serait-ce que pour ne pas contaminer les autres offres qui seraient ouvertes sur ce poste (cf. annexe 6).

9. La réparation des fichiers

> **Vade-mecum, § 10.4 :** […] l'intérêt de l'acheteur est de mettre en œuvre un programme de réparation du document contaminé. Deux situations peuvent en résulter : le document retrouve son intégrité initiale et la procédure suit son cours ; en revanche, si le document ne peut pas être réparé ou que sa réparation ne lui restitue pas son intégrité, la personne publique n'aura d'autre choix que de considérer ce document comme nul ou incomplet

Si elle ne décide pas de procéder à un archivage de sécurité sans lecture du document contaminé, la collectivité publique peut tenter de réparer le fichier en demandant à son anti-virus de supprimer le virus détecté. Le document ainsi décontaminé pourra être examiné.

Toutefois, il convient de faire extrêmement attention à l'usage de l'anti-virus pour réparer un fichier. En effet, cela entraîne une modification du fichier, qui n'est donc plus l'original transmis par l'entreprise. De ce fait, **toute signature électronique associée à ce fichier sera invalide à l'issue de la réparation**.

En outre, si la réparation ne réussit pas totalement, la collectivité publique ne pourra exploiter cette offre. Incomplète ou illisible partiellement, l'offre devra vraisemblablement être rejetée.

10. La demande de pièces complémentaires dans les candidatures

Lors des phases de candidature, la collectivité publique a la possibilité de demander aux soumissionnaires l'envoi de pièces manquantes. Un document réputé non reçu parce qu'infecté par un virus remplit ces conditions, et la collectivité publique peut donc demander que le document lui soit envoyé de nouveau, une fois désinfecté par l'entreprise.

Si elle souhaite utiliser cette possibilité, la collectivité publique doit opter pour un archivage de sécurité sans lecture du document, et donc sans tentative de réparation.

ANNEXE 6 : l'ouverture des plis et les virus

1. Observation liminaire

Ce document est destiné à une utilisation opérationnelle. Il ne fait pas une analyse de risque et décrit uniquement l'environnement Windows.

Configuration cible décrite dans deux des sites consultés :

Une entreprise envoie ses réponses à une plate forme en les chiffrant. La confidentialité est obtenue en utilisant la clé publique publiée par la plate forme pour l'appel d'offre auquel il est répondu. La PRM reçoit les offres chiffrées sur son poste de travail.

Dans cette configuration il est possible d'observer :

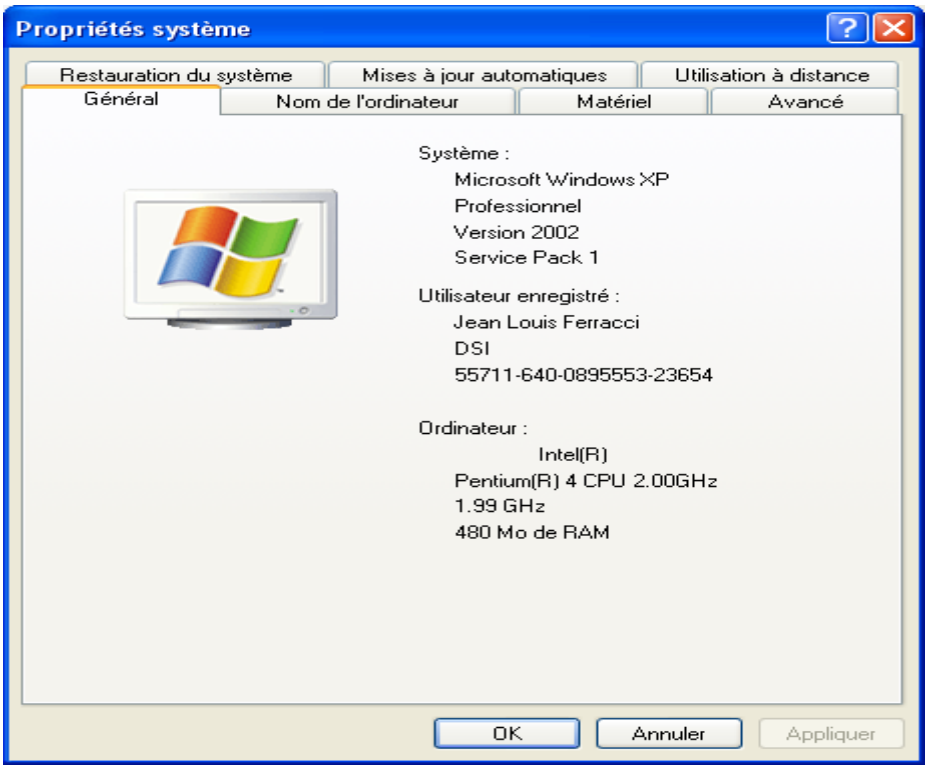
Que la plate forme ne pourra être accusée d'avoir introduit des virus dans les documents (sauf la remarque liée au séquestre des clés de chiffrement). Que seules deux entités pourront donc se rejeter la responsabilité de la contamination, à savoir l'entreprise qui a créé puis chiffré les documents – ils ont pu être contaminés lors de la création - et la personne publique qui seule a pu les déchiffrer – ils ont pu être contaminés après le déchiffrement. Toute la sécurité de l'exercice pour la PRM devra consister à décrire une procédure sans faille, à en conserver les traces et à enregistrer cela dans le procès verbal de la commission d'appel d'offres. Ce Procès-verbal devrait préciser la séquence indiquée ci-dessous.

2. Etat du poste de travail avant la procédure : description du contexte

2.1 Date système à jour

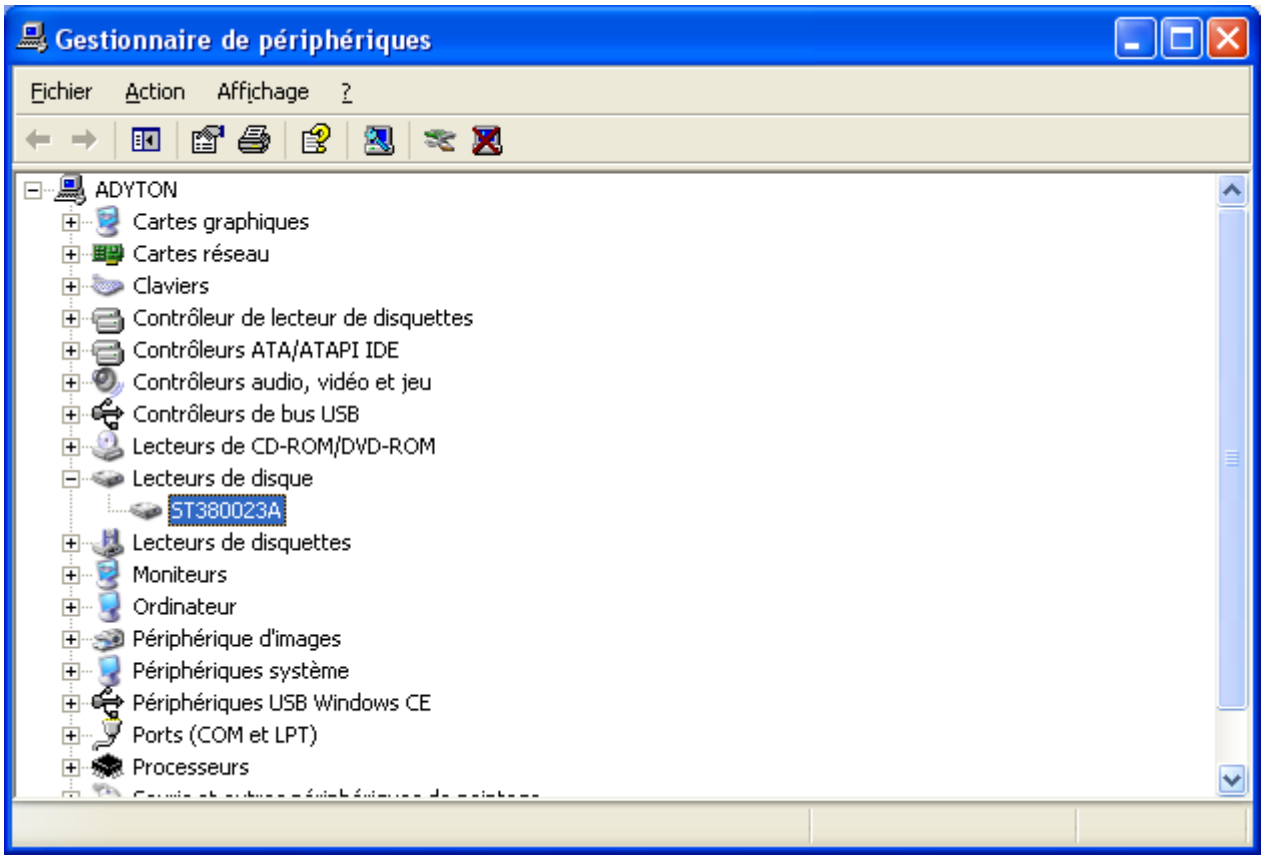
2.2 Marque et version du système d'exploitation du poste de travail

- Doit constituer l'annexe 1 du procès-verbal



2.3 Nom du poste et éléments de stockage

- Cf. nombre de disques ;
- Doit constituer l'annexe 2 du procès-verbal



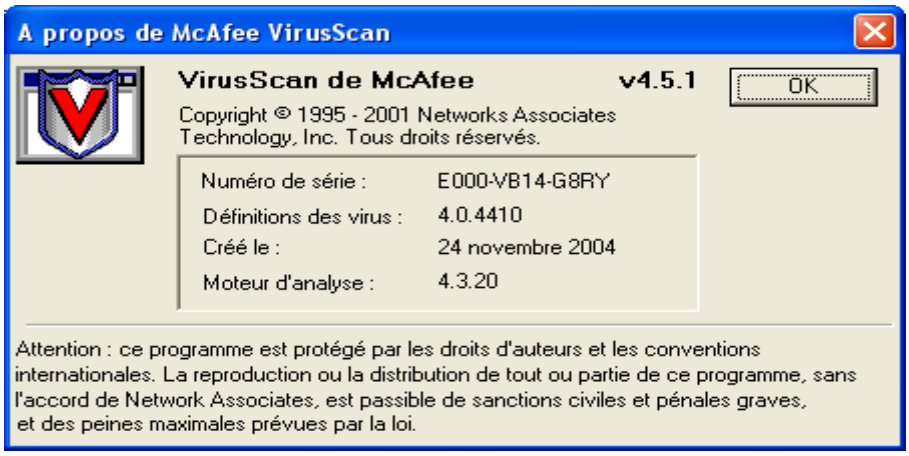
2.4 Connexion ou non à un réseau

- Un poste isolé avec, selon l'importance du marché, un processeur non Centrino serait la meilleure solution ;
- Doit constituer l'annexe 3 du procès-verbal.

2.5 Antivirus installé sur le poste de travail

- Marque, numéro de série, numéro de série du logiciel, version du moteur et version de la définition des virus [18]
- Doit constituer l'annexe 4 du procès-verbal.

[18] Les illustrations sont fournies à titre d'exemple. Il ne s'agit donc pas d'encouragements implicites à l'usage des logiciels qui ont permis de les réaliser.



2.6 Impression de la page du site de l'éditeur de l'anti-virus

- Celle où sont publiées les références de la dernière version de mise à jour. Cette page est datée, numérotée et contre signée par la PRM.
- Doit constituer l'annexe 5 du procès-verbal.

NB : la comparaison entre la publication et la version possédée montre que le poste est au meilleur niveau de défense possible.

2.7 L'impression des journaux de l'antivirus (préalablement remis à zéro) :

Celui de la mise à jour (Avec MacAfee : C:\Program Files\Network Associates\VirusScan\Update.txt)

- Doit constituer l'annexe 6 du procès-verbal

29/11/2004	*11:50*	*SYSTEM*	*ADYTON*	*La tâche AutoUpdate a démarré.*
29/11/2004	*11:54*	*SYSTEM*	*ADYTON*	*Les fichiers .DAT ont été mis à jour de la version 4410 à la version 4410.*

Celui de la vérification des fichiers : (extrait) annexe 7 du procès-verbal

29/11/2004	*10:31*	*Analyse démarrée*	*ADYTON\JLF*	*Analyse à la demande*
29/11/2004	*10:31*	*Paramètres d'analyse*	*ADYTON\JLF*	*Paramètres d'analyse courants :*
29/11/2004	*10:31*	*Paramètres d'analyse*	*ADYTON\JLF*	*Taille du fichier d'activité limitée à 100 ko. : 0*
29/11/2004	*10:31*	*Résumé d'analyse*	*ADYTON\JLF*	*Fichiers déplacés : 0*
29/11/2004	*10:31*	*Analyse terminée*	*ADYTON\JLF*	*Analyse à la demande*

3. Ainsi à la fin de la première étape la PRM peut prouver

- qu'elle a mis le poste décrit au meilleur niveau possible de protection ;
- qu'elle a mis en œuvre les outils sur le poste ;
- que le poste de travail est sain.

4. Transfert des fichiers sur le poste de travail

Liste des fichiers transférés :
Noms, tailles, dates
La liste (éventuellement impression d'écran du sous répertoire) est datée et signée par la PRM**.**

- Doit constituer l'annexe 8 du procès-verbal.

5. Ouverture des plis :

Le déchiffrement devrait se faire de façon unitaire, les fichiers déchiffrés et qui se seront révélés sains devant être transférés sur un autre support avant de déchiffrer un second fichier. Ceci afin d'éviter une contamination.

La procédure ci-dessous doit donc être répétée autant de fois qu'il y aura de déchiffrement.

Lancement du déchiffrement dans un sous répertoire ad hoc différent de celui dans lequel sont déposés les fichiers chiffrés :

Liste des fichiers déchiffrés :

Nom, taille, date
La liste (éventuellement impression d'écran du sous répertoire) est datée et signée par la PRM**.**

- Doit constituer l'annexe 9 du procès-verbal.

La PRM s'assurera que tous les fichiers chiffrés sont bien déchiffrés. Une règle de nommage serait d'ailleurs la bienvenue afin que les entreprises puissent attribuer des noms permettant d'assurer un suivi (par exemple le nom d'un fichier chiffré est identique à celui du nom de celui en clair, sauf l'extension, etc.).

Pour chaque fichier déchiffré, et aussitôt après, un test prophylactique doit être réalisé.

- L'ensemble des tests unitaires constitue l'ANNEXE 10 du procès-verbal

Exemple de test unitaire (extrait) :

29/11/2004	15:08	Analyse démarrée	ADYTON\JLF	Analyse à la demande
29/11/2004	15:08	Paramètres d'analyse	ADYTON\JLF	Paramètres d'analyse courants:
29/11/2004	15:08	Paramètres d'analyse	ADYTON\JLF	

R:\DÉMATÉRIALISATION MARCHÉS PUBLICS\COMMENTAIRES SUR CHIFFREMENT.DOC

29/11/2004	15:08	Résumé d'analyse	ADYTON\JLF	Résumé de l'analyse
29/11/2004	15:08	Résumé d'analyse	ADYTON\JLF	Fichiers analysés : 1
29/11/2004	15:08	Résumé d'analyse	ADYTON\JLF	Fichiers infectés : 0
29/11/2004	15:08	Résumé d'analyse	ADYTON\JLF	Fichiers nettoyés : 0
29/11/2004	15:08	Résumé d'analyse	ADYTON\JLF	Fichiers supprimés : 0
29/11/2004	15:08	Résumé d'analyse	ADYTON\JLF	Fichiers déplacés : 0
29/11/2004	15:08	Analyse terminée	ADYTON\JLF	Analyse à la demande

L'ensemble des fichiers chiffrés et déchiffrés, les fichiers infectés ainsi que les journaux pourrait ensuite être stocké sur un cédérom qui serait scellé mécaniquement (passage d'un lien dans le vide central et réunions des deux extrémités par un moyen de scellement quelconque (plomb, cire, scellés plastiques, etc.) et/ou contenu dans une enveloppe à ouverture inviolable, et conservé aux fins de preuves en annexe au procès-verbal.

ANNEXE 7 : conduite à tenir en cas d'indisponibilité inopportune de la plate-forme et autres incidents

La plupart des incidents susceptibles d'affecter une procédure dématérialisée sont de même nature que ceux qui sont déjà possibles avec les procédures manuelles : compromission d'informations confidentielles, ouverture prématurée de certaines offres, altération ou perte de documents, litiges sur l'heure de remise des offres etc.

Deux différences importantes cependant existent entre les procédures manuelles et les procédures dématérialisées : d'une part les procédures automatisées, quand elles sont bien conçues du moins, réduisent le risque d'erreur humaine, et d'autre part – et inversement - la confiance qu'inspirent naturellement les procédures automatisées, jointe à leur opacité pour l'utilisateur, rendent plus difficile la détection des incidents éventuels et peuvent faciliter les malveillances par qui en maîtriserait les mécanismes. Des moyens manuels et automatiques supplémentaires doivent donc être prévus et appliqués pour assurer et contrôler la sécurité. Ceci étant, puisque la plupart des incidents éventuels reste de même nature qu'avec les procédures manuelles, la façon d'en limiter les conséquences est similaire.

Toutefois les procédures automatisées sont susceptibles de connaître plusieurs types d'incidents qui n'affectent pas les procédures manuelles : il s'agit de :

- la présence de virus et autres codes malveillants dans les fichiers échangés ; ces incidents ont été traités aux annexes 5 et 6 ;
- l'indisponibilité de la plate-forme au moment de la remise des offres ou candidatures, que cette indisponibilité soit accidentelle (incendie, perte d'alimentation électrique, coupure des télécommunications, erreur de manipulation des opérateurs…) ou due à la malveillance (déni de service, ou toute autre attaque sur la plate-forme) ;
- de l'indisponibilité des connexions à internet, notamment si elles sont dues au fournisseur d'accès à internet (FAI) .

1. Indisponibilité ou engorgement de la plate-forme au moment de la remise des offres

On peut évidemment rapprocher ce type d'incident de perturbations graves dans les services postaux : les entreprises qui ont confié leur offre à La Poste en sont affectées, alors que celles qui ont déposé leur offre par porteur en sont protégées. Toutefois, d'une part les perturbations dans les services postaux sont généralement largement connues dans le public quand elles se produisent, et d'autre part les entreprises ont confié leur courrier à La Poste en tenant compte des délais postaux : dans beaucoup de cas par conséquent, l'entreprise peut probablement, si elle craint que La Poste n'achemine pas son offre en temps voulu, respecter les délais imposés en remettant une copie de son offre par porteur.

Il n'en est pas de même pour une procédure dématérialisée :

- l'indisponibilité de la plate-forme n'est pas forcément publique, et d'ailleurs, pour l'entreprise qui n'arriverait pas à transmettre son offre, il peut ne pas être facile d'en connaître la cause, laquelle peut être propre à l'entreprise, à son fournisseur d'accès internet, ou à tout autre point de la chaîne qui permet d'acheminer l'offre ;
- pour profiter au mieux des avantages de la dématérialisation, les entreprises auront tendance à remettre leur offre au dernier moment ;
- et enfin le choix de la dématérialisation pour un marché, par l'entreprise, est irréversible : de toutes façons, elles ne peuvent plus remettre leur offre de façon non dématérialisée.

En cas d'indisponibilité ou d'engorgement inopportuns de la plate-forme il est donc indispensable :

- que la personne publique en soit immédiatement avertie par les administrateurs de la plate-forme, qui lui indiquent la durée probable de l'indisponibilité ou dégradation des conditions d'accès et la tiennent au courant de la situation ;
- que la PRM prévienne rapidement les entreprises qui ont choisi la procédure dématérialisée, par tous les moyens possibles (courrier électronique, téléphone, télécopie…) ;
- qu'elle leur donne les consignes nécessaires ; ce peut être une solution de secours dont les modalités auront été annoncées dans le dossier de consultation, comme l'envoi des offres à la personne publique par courrier recommandé chiffré ; ce peut être aussi, plus simplement, une extension du délai de remise des offres qui permette à tous les concurrents, qu'ils aient ou non choisi la dématérialisation, de remettre une nouvelle offre s'ils le souhaitent.

Ceci exige donc que :

- la PRM tienne la liste exhaustive des entreprises qui sont susceptibles de répondre, c'est à dire qui ont chargé le DCE ;
- qu'elle ait prévu des procédures pour les prévenir et leur donner ses consignes ; ceci doit être fait de façon fiable, c'est à dire d'une part que les entreprises doivent pouvoir authentifier l'origine de ces informations et consignes, pour éviter les mauvaises plaisanteries et malveillances qui viendraient aggraver les conséquences de l'indisponibilité, et d'autre part que la PRM puisse démontrer qu'elle a contacté toutes les entreprises concernées.

2. Indisponibilité des connexions à internet dues au FAI

Pour diverses raisons, les connexions à internet peuvent être indisponibles du fait du FAI, par exemple par suite d'une fausse manœuvre de sa part[19]. Les utilisateurs doivent donc être attentifs aux anomalies éventuelles qu'ils constateraient dans leur connexion à Internet (accusés de réception qui ne reviennent pas, impossibilité d'accéder à la plate-forme etc.) . S'ils détectent une anomalie, ils doivent, après s'être assurés que cette anomalie n'est pas de leur fait (ou de celui de l'opérateur de télécommunications proprement dit), contacter leur FAI pour obtenir des explications et une indication des délais de rétablissement. Pour le cas où ces délais ne seraient pas compatibles avec ceux de la procédure, ils doivent avoir prévu la possibilité d'accéder à internet depuis un autre FAI.

[19] L'exemple d'un incident réel côté prestataire de service illustre la nature du risque ; il concerne l'inscription, à tort, du serveur de mail de ce prestataires sur la liste des serveurs qui envoient des courriers non sollicités (spam).
Ce prestataire a mis à jour son serveur de messagerie et l'a rendu visible sur Internet pendant cette intervention ; un spammeur a profité de cette occasion pour l'utiliser comme relais. Les sites anti-spam ont détecté ce serveur de messagerie comme un serveur de spam et ont « blacklisté » son adresse IP. Les opérateurs qui référencent ces sites ont pris en compte cette information.
La société A qui possède un serveur de messagerie hébergé chez cet opérateur, ne pourra plus adresser son offre alors que la société B accédera au site sans problème. Comment la société A peut-elle attribuer ce problème à son prestataire, et lui en faire porter la responsabilité ?

ANNEXE 8 : archivage

Certains documents d'une procédure de marchés publics doivent être conservés sur des durées si longues qu'ils pourraient devenir illisibles, bien avant la fin de la durée légale d'archivage, par les matériels et les logiciels disponibles. Comme le prescrit le vade-mecum juridique, il convient donc de les transcoder dans un « format pivot », choisi pour rester utilisable sur la période nécessaire et de s'assurer de plus que les supports utilisés restent utilisables aussi longtemps que nécessaire[20].

Ceci pose des problèmes particuliers pour les documents signés :

- tout transcodage effectué pour éviter l'obsolescence technique modifie le fichier dématérialisé et donc invalide sa signature originelle, même s'il ne modifie pas le résultat de sa rematérialisation ;
- de plus une signature valide à un instant donné ne le reste pas indéfiniment, puisque le certificat se périme un jour, normalement bien avant la fin de la période réglementaire d'archivage, et ce même s'il n'y a pas eu de transcodage.

Des précautions doivent donc être prises pour être en mesure d'attester que la signature était valable au moment où elle a été apposée et que le fichier transcodé contient exactement les mêmes informations que celui qui a été originellement signé .

Toutefois il est raisonnable de penser que des fichiers informatiques de format courant restent lisibles pendant plusieurs années. Ils devront en outre être enregistrés sur des supports comme des CD-ROM (une durée de cinq ans est en général possible, aussi bien vis à vis de l'obsolescence des formats de fichiers que vis à vis de la dégradation des CD-ROM). Par conséquent, on peut se contenter dans un premier temps, d'archiver les fichiers afférents à la procédure sur un CD-ROM, avec la signature qui est apposée, pour ceux qui sont signés, et en précisant alors que leur signature était valable au moment où elle a été apposée ; si la PRM dispose d'un certificat, il est utile qu'elle signe elle-même ces archives ; sinon elle doit prendre les précautions nécessaires pour que ces archives ne puissent être contestées. Il est par ailleurs indispensable que le gravage des dossiers sur un CD-R s'accompagne de celui des métadonnées permettant de retrouver les dossiers :

- Identification de l'acheteur public et de l'entreprise
- Numéro du marché
- type de marché : fournitures et courant / services / travaux
- type de la procédure de mise en concurrence
- objet du marché (texte libre)
- numéro du lot
- suivant les types de marchés : dates
    - date et heure de l'envoi de l'avis de pré-information
    - date et heure de l'envoi de l'APPC
    - date et heure de l'envoi du rectificatif
    - date et heure du retrait du DCE
    - date et heure de l'envoi de la lettre de consultation
    - date et heure de réception des candidatures
    - date et heure de réception des offres
    - date et heure d'ouverture des plis
    - date et heure de notification
    - date de clôture de la procédure.

[20] Voir dans le vade-mecum la partie 13 ainsi que l'annexe 1 (propositions d'organisation des fichiers, de structuration des informations, nommage des fichiers, formats des fichiers) et l'annexe 2 (modalités de transfert sur une plate-forme d'archivage électronique).

Ces différentes clés d'accès doivent être reprises dans un fichier simple type Excel permettant de retrouver facilement les données avec l'indication supplémentaire du numéro du CD-R permettant de faire le lien entre le CD-R et les marchés qui y sont gravés.

Par ailleurs, il est conseillé de ne graver sur un CD-R que les marchés ayant la même durée de conservation de manière à faciliter leur gestion dans le temps : grouper les candidatures et les offres non retenues (délai de conservation 5 ans), les marchés de fournitures. (délai de 10 ans), les marchés de travaux (30 ans). Pour la détermination des délais, il convient de se reporter à la partie 13 de l'annexe.

Dans ce cadre, je vous rappelle que l'élimination par exemple au terme d'un délai de 5 ans des candidatures et offres non retenues, doit être soumis, comme pour les archives papier, aux services publics d'archives

Cette solution ne peut être que temporaire, et il ne faut donc pas oublier qu'il sera nécessaire un jour de transcoder ces archives et prendre alors les précautions évoquées ci-dessus, que l'état de l'art, à l'époque, devrait rendre alors plus faciles.

Concernant la production et la conservation de ces CD-R, voir l'annexe 9, qui est la synthèse d'une recommandation sur le sujet, émanant de la direction des Archives de France : choix des CD-R, choix d'un graveur, mode de gravure, modalités de conservation, surveillance et renouvellement des CD-R., avec la production d'un double jeu de CD-R conservés en deux endroits distants.

Comme pour l'archivage des documents papiers, ces archives électroniques doivent être conservées dans de bonnes conditions physiques et à l'abri des accidents et altérations de tout ordre. Le volume réduit des archives électroniques rend d'ailleurs cette conservation plus facile.

ANNEXE 9 : recommandations de la direction des archives de France relatives à la gravure, à la conservation et à l'évaluation des CD-R

Ce mémento pratique reprend les éléments principaux des Recommandations *mais son utilisation requiert la lecture préalable du document complet.*

1. Le choix d'un CD-R

Choisir des disques possédant les caractéristiques suivantes :

- film métallique réfléchissant en or de préférence ;
- couche de colorant organique phtalocyanine ou azoïque ;
- capacité 74 ou 80 minutes ;
- modèle dédié à la conservation de longue durée ;
- conditionnement en boîtiers rigides.

Acheter de préférence en une seule fois la quantité de disques nécessaire pour une année, plutôt que de petites quantités.

2. Le choix d'un graveur

Si le choix se porte sur un graveur externe, il est nécessaire de disposer d'une liaison rapide entre le graveur et le poste informatique.

3. Le mode de gravure

Remplir le disque à 90 % de sa capacité au maximum.

Sélectionner les options suivantes dans le logiciel de gravure :

- format CD de données (CD-ROM mode 1 ou CD-ROM XA mode 2) ;
- système de fichiers ISO 9660 niveau 2 ;
- enregistrement en une seule session.

Remplir la zone de description du disque (nom de volume, nom de l'éditeur, nom du responsable de l'enregistrement, date).

Réaliser d'abord une image du disque, à graver dans un second temps.

Eviter de graver à trop grande ou à trop basse vitesse : une vitesse de 16 x ou 12 x convient généralement.

Ne pas effectuer d'autres tâches sur le poste informatique pendant la gravure.

Lors de chaque changement de lot de disques, de graveur ou de lieu de production, il convient de vérifier l'adéquation du couple disque / graveur (calibration) :

- enregistrer un disque à 95 % de sa capacité et à la vitesse envisagée ;
- vérifier le disque bit par bit ;
- tester ou faire tester le CD-R gravé, au moyen d'un appareil spécialisé appelé analyseur.

De temps en temps, vérifier quelques disques gravés, au moyen d'un logiciel de test par exemple.

Pour permettre une traçabilité de la production, garder, pour chaque CD-R produit, les informations suivantes :

- la cote du disque ;
- la date de la gravure ;
- la provenance du disque (marque, caractéristiques techniques, éventuellement numéro de série) ;
- le modèle et le numéro de série du graveur ;
- la version du « firmware » ou micrologiciel du graveur ;
- le nom et la version du logiciel de gravure ;
- la vitesse de gravure ;
- le nom du responsable de la gravure (notamment dans le cas d'une prestation externe).

Les disques produits dans des conditions homogènes forment des lots.

4. Les conditions de stockage et de manipulation à respecter

Conditions de stockage à respecter :

- température comprise entre 16 et 23 °C ;
- taux d'humidité relative compris entre 30 et 50 % ;
- éviter les variations brusques de température et d'humidité ;
- éviter une exposition à la lumière du jour ;
- éviter une exposition à la poussière.

Tenir le disque par l'anneau central, sans jamais toucher la zone enregistrée.

Si le disque est sale, le nettoyer par exemple avec un chiffon non pelucheux et de l'eau savonneuse, en effectuant des mouvements du centre vers la périphérie.

Pour légender le CD, il est possible d'utiliser :

- un feutre à pointe douce, avec une encre à base d'eau ou éventuellement d'alcool (feutres spéciaux pour CD) ;
- une imprimante à jet d'encre, à condition que le disque soit recouvert d'une couche adaptée.

Eviter absolument les étiquettes, les crayons à pointe fine et les encres contenant des solvants.

5. Surveiller et renouveler les CD-R

La surveillance des CD-R gravés s'effectue par lots.

Selon la taille des lots, il peut être plus intéressant de réaliser des tests (lots importants) ou de recopier les disques selon une périodicité fixe (petits lots).

Si l'on choisit d'effectuer des tests, la périodicité peut être comprise entre un an et demi et cinq ans.

Les tests doivent porter sur un échantillon du lot considéré. La taille de l'échantillon dépend de la taille du lot, selon des règles statistiques (par exemple, 80 disques pour un lot de 1 000, 200 pour un lot de 4 000 ; voir tableau complet au 6.3.2 des recommandations).

Les tests doivent être effectués, en interne ou par sous-traitance, au moyen d'un analyseur.

Si une partie de l'échantillon est de qualité insuffisante, l'ensemble de lot doit être transféré sur un nouveau support.

ANNEXE 10 : points concernant la sécurité dans un marché d'hébergement

Dans la cas où la personne publique fait héberger le service de dématérialisation de ses marchés publics, la sécurité de cet hébergement doit être spécifiée au marché passé au prestataire. Les clauses-types que proposent les prestataires abordent en général ce sujet, mais il appartient de toutes façons à la personne publique de le vérifier, pour, si elle l'estime nécessaire, modifier et compléter ces clauses-types.

Les principaux points à traiter dans le contrat d'hébergement concernent les limites de responsabilité entre le prestataire et son client, les services rendus, l'assurance qualité du prestataire, les modalités de sortie du marché, le suivi et le contrôle de l'exécution des prestations, et la charte déontologique à laquelle s'engage le prestataire. Ce document a pour objet de lister les points à examiner dans le contrat d'hébergement.

1. Responsabilité

La clause de responsabilité détermine les limites de responsabilités entre le prestataire et la personne publique. En fonction de l'architecture technique de la solution retenue, il sera nécessaire de préciser le périmètre de responsabilité des acteurs sur l'ensemble des domaines et notamment sous l'angle sécurité.

En particulier le prestataire devra indiquer s'il fait appel à des sous-traitants, et la nature de ses relations avec ces tiers sur le plan des responsabilités. Le montant maximum des indemnisations que le prestataire accepte de verser à son client en cas d'anomalie ou d'erreur dans ses prestations devra être spécifié. Sans que ce soit une obligation contractuelle, il est souhaitable que le prestataire communique à son client la police d'assurance qu'il a souscrite pour se protéger des conséquences de ces anomalies et erreurs.

2. Convention de services

La convention de services décrit la nature des services offerts dans le cadre du contrat entre la personne publique et le prestataire (SLA – « Service Level Agreement » en anglais) et doit comprendre :

2.1 Les objectifs de services

Dans le processus de dématérialisation, l'interopérabilité nécessaire entre les systèmes d'information du prestataire et celui de la personne publique peut conduire à des risques non maîtrisés par l'une ou l'autre des parties. La description exhaustive des services fournis par le prestataire permet de déterminer le périmètre de responsabilité entre les parties :

- disponibilité de l'infrastructure technique, des accès et des débits ;
- gestion de la confidentialité des offres lors de leur hébergement sur le serveur ;
- gestion de l'horodatage ;
- engagement sur la gestion des incidents pendant les différentes phases de la consultation (support, procédures prédéfinis, etc.) ; information de la personne publique en cas d'indisponibilité ou de saturation ;
- tableaux de bords et indicateurs.

La description des moyens mis en œuvre sur le plan organisationnel et technique pour garantir ce niveau de service sera présentée dans le Plan d'Assurance Qualité.

2.2 Politique de sécurité

Il existe des risques inhérents à la mise en œuvre de la dématérialisation des marchés publics. La communication de la politique sécurité couvrant les aspects techniques et organisationnels de mise en

œuvre sur le plan sécurité par le prestataire doit permettre à l'acheteur public d'évaluer en terme de moyens les mesures prises pour réduire ces risques.

2.3 Gestion du changement

Les évolutions techniques du service peuvent perturber l'exécution des appels d'offres. L'infrastructure technique en place nécessite des mises à jour des logiciels et des matériels qui peuvent entraîner une interruption de service. Le niveau de disponibilité offert mais surtout les conditions dans lesquelles les interruptions volontaires du service sont pratiqués doivent être précisés. Il s'agit par exemple de ne pas arrêter le service moins de 24h avant la date limite de remise de propositions pour un appel d'offres et dans tous les cas de communiquer préalablement ces arrêts aux utilisateurs et clients du service.

2.4 Conformité légale et réglementaire

Le respect de la réglementation et des lois est un élément primordial du service de dématérialisation :

- conditions Générales d'Utilisation du service ;
- réglementation sur les données ;
- réglementation sur la cryptographie.

3. Plan d'Assurance Qualité (PAQ)

Le PAQ détermine les moyens mis en œuvre pour satisfaire la convention de services. Les différents processus et mesures de sécurité prises devront être formalisés dans ce document en terme :

- d'acteurs et de responsabilité vis à vis des différentes phases de l'achat public ;
- de description des procédures de suivi et de contrôles en place pour satisfaire les obligations décrites dans la convention de services (comité de pilotage, audit, etc.).

4. Réversibilité /transférabilité

A échéance du marché, la personne publique a la capacité de changer de prestataire. Dans ce cadre les conditions de transférabilité doivent être précisées dans le contrat initial. Elle concerne non seulement les affaires encore en cours à l'échéance du marché, mais aussi tous les éléments éventuellement archivés par le prestataire et les éléments spécifiques à la personne publique mis en œuvre par le prestataire durant la vie du contrat (par exemple le paramétrage, les droits attribués aux différents agents de la personne publique etc.).

5. Continuité du service

La disponibilité du service est primordiale dans certaines phases du processus d'achat public. il s'agira de s'assurer de la continuité de service en cas de sinistre du prestataire. Il décrira les procédures mises en place pour assurer cette continuité :

- gestion de la communication aux soumissionnaires et à l'acheteur public ;
- plan de reprise d'activité ;
- nature et fréquences des tests et contrôles de ce plan.

6. Suivi /contrôle

Il convient de s'assurer que le prestataire respecte notamment les exigences de sécurité reprises dans la convention de services. Ce point concerne les règles de gestion du marché (ex : comité de pilotage) et les moyens pour s'assurer de la conformité (ex audit).

Cet audit doit porter sur le respect des points suivant :

- convention de service (outils, moyens et procédures mis en œuvre par le prestataire pour l'exécution du marché) ;
- politique de sécurité ;
- continuité du service ;
- maintien des conditions de réversibilité ;
- conformité à la réglementation sur les marchés publics, les données personnelles et la cryptographie.

Les conditions dans lesquelles l'exécution du marché ne serait pas conforme à la convention de service ou au PAQ devront être décrites ainsi que les conditions de résiliation du marché de prestations par la personne publique.

7. Charte déontologique

Le prestataire de service peut faire partie d'un groupe dans lequel certaines sociétés pourraient soumissionner dans le cadre des prestations . Le risque existe dans ce cas de conflit d'intérêt et de litiges. Il convient de s'assurer dans ce cas que l'égalité de chance devant l'achat public est respectée par la mise en place de règles déontologiques. Le prestataire décrira les procédures de contrôle interne garantissant le respect de ces règles.

ANNEXE 11 : acquisition d'un progiciel

Si la personne publique décide d'opérer elle-même la plate-forme de dématérialisation et acquiert pour cela un progiciel, elle doit veiller à ce que les fonctionnalités de sécurité du progiciel permettent de prendre les mesures de sécurité nécessaires.

De plus, et comme pour tous les progiciels, elle doit obtenir de l'éditeur des engagements sur les points suivants :

- soutien technique : collecte des incidents constatés, procédures de contournement et de correction des défauts et anomalies ;
- évolutions du progiciel, rendues nécessaires par exemple par une évolution de la réglementation ou la correction d'erreurs : dans quelles conditions l'éditeur proposera-t-il les évolutions ?
- évolutions du progiciel à l'initiative de l'éditeur : dans quelles conditions le client peut-il, s'il le souhaite, continuer d'utiliser l'ancienne version ?
- qualité de la documentation, pour les exploitants et les utilisateurs ;
- formation des exploitants et des utilisateurs ;
- assistance aux exploitants et aux utilisateurs : fonctionnement d'une « hot-line » par exemple ;
- réversibilité :

    - dans quelle conditions sera-t-il possible à la personne publique de prendre ultérieurement un autre progiciel (par exemple, normalisation des formats de fichiers, pour éviter des transcodages etc.) ?
    - dans quelles conditions, en cas de défaillance de l'éditeur ou d'abandon du produit, la personne publique pourra-t-elle continuer à l'exploiter ? En particulier, l'éditeur devra préciser dans quelles conditions les codes source, la documentation, les bibliothèques et tous les autres éléments nécessaires pourront être rendus accessibles à la personne publique pour qu'elle puisse en assurer elle-même le soutien, ou en charger une autre société, si l'éditeur ne pouvait ou ne voulait plus le faire.

ANNEXE 12 : réflexions générales sur les attaques informatiques

Quelque possible voire facile qu'elle soit, une attaque sur un système informatique demande toujours quelques compétences et comporte un certain risque pour l'attaquant. Il faut donc avoir une idée des attaquants à redouter, de leurs compétences, des moyens qu'ils pourraient utiliser et des risques qu'ils sont prêts à prendre ; ces risques sont probablement fonction des profits que les attaquants espèrent retirer de leur malveillance. Ils dépendent, également, de la probabilité que l'attaquant soit détecté et identifié, et des conséquences qu'aurait pour lui le fait d'être découvert.

Pour l'attaquant, les motivations générales, qui ne sont d'ailleurs pas spécifiques au cas des marchés dématérialisés, ni même aux systèmes informatisés, peuvent être :

- la gloriole d'avoir réussi ce qu'il pense être une exploit : c'est ce qui semble inspirer les « hackers » de passage et autres auteurs de virus ;
- la malveillance aveugle, le vandalisme ;
- la méchanceté, la vengeance, de la part de personnes proches du propriétaire du système : il arrive en effet que des employés ou anciens employés y recourent, et d'ailleurs toutes les statistiques sur les malveillances informatiques montrent que les attaques internes sont les plus fréquentes, après bien sûr les virus ;
- la cupidité : ce serait le cas, par exemple, d'une entreprise qui s'efforcerait de gêner ou d'espionner ses concurrents dans un appel d'offres ; c'est souvent aussi une motivation des malveillances internes ; c'est aussi une motivation qui apparaît de plus en plus fréquemment dans les attaques de « hackers », lesquels s'efforcent d'obtenir des renseignements confidentiels ou procèdent à des chantages, sous la menace d'attaques informatiques[21].

Bien évidemment, des attaques peuvent être menées qui associent plusieurs de ces motivations : par exemple des « hackers » proposent de louer leurs services à des entreprises criminelles, des entreprises malveillantes s'assurent la coopération d'employés de leurs concurrents ou partenaires qui seraient mécontents, cupides ou vulnérables à un chantage.

On quantifie comme suit le niveau de compétences nécessaire pour conduire une attaque :

- faible si des «hackers» le font couramment, ou s'il suffit de prendre avantage d'une organisation (de la personne publique ou de l'entreprise) gravement déficiente ;
- moyen s'il faut en plus exploiter une imprudence fortuite, si une personne à l'intérieur de l'organisation enfreint sciemment les consignes (on suppose que ces personnes sont a priori de confiance, c'est donc que la confiance a été mal placée), s'il faut mettre en œuvre des moyens importants, faire de « l'ingénierie sociale » ;
- fort s'il faut mettre en œuvre des moyens très importants, techniques et autres comme la corruption d'une personne de confiance.

Puisque la plupart des outils et techniques employées dans les systèmes de dématérialisation (utilisation d'internet, de navigateurs ordinaires, de courrier électronique, de signature électronique, de chiffrement, de formats de fichiers courants etc.) sont d'un usage courant pour de nombreux autres systèmes :

- d'une part on imagine difficilement des attaques dont les méthodes et techniques seraient spécifiques à ces systèmes de dématérialisation, même s'ils peuvent attirer des malveillances dont les motivations seraient bien spécifiques (espionner des concurrents, corrompre leur offre, les empê-

[21] C'est ainsi que les sites internet de jeux en ligne sont fréquemment soumis à des chantages exigeant des paiement sous la menace d'attaques en déni de service, attaques qui causeraient évidemment à ces sites des dommages importants.

cher de remettre leur offre, faire annuler une procédure, embarrasser la personne publique par des incidents spectaculaires etc.) ;

- et d'autre part les systèmes de dématérialisation sont a priori exposés à toutes les attaques que l'on constate quotidiennement ; ils doivent donc s'en protéger pour ramener les risques à un niveau de sécurité acceptable.

Le Club de la sécurité des systèmes d'information français (CLUSIF) publie chaque année un panorama de la cybercriminalité qui donne une idée de la variété des attaques et de leur nocivité.

Rapport 2004 : https://www/clusif.asso.fr/index.asp
Années précédentes : https://www.clusif.asso.fr/fr/production/sinistralite/

ANNEXE 13 : précautions à prendre avec le courrier électronique

Le courrier électronique apporte en général une commodité d'emploi et une rapidité très appréciées. Il faut cependant être conscient qu'il n'apporte aucune garantie de sécurité : il peut être lu et modifié par des tiers (pas de confidentialité ni d'intégrité), son émetteur n'est pas connu de façon fiable (pas d'opposabilité), les délais de remise ne sont pas garantis et la remise elle-même n'est pas garantie non plus (pas de disponibilité). Enfin il ne peut pas non plus être tracé de façon fiable (pas de traçabilité) ; toutefois, s'il est signé, son intégrité et son opposabilité sont assurées et s'il est chiffré, sa confidentialité l'est aussi, dans la limite, bien sûr de ce que permettent les procédures et les procédés utilisés et avec certaines précautions cependant, car il se peut que certains pare-feux refusent de laisser passer les courriers signés ou chiffrés.

Des prestataires proposent des services de courrier électronique recommandé et fournissent un accusé de réception. Ces services assurent la traçabilité, sans avoir cependant la valeur juridique des courriers recommandés postaux (lesquels d'ailleurs prouvent simplement qu'un courrier a été envoyé et reçu, mais n'attestent rien quant au contenu du courrier). Par contre il n'existe aucun moyen technique de garantir la disponibilité du courrier électronique.

L'utilisation du courrier électronique ordinaire doit donc être accompagnée de précautions :

- ne pas l'utiliser sans chiffrement pour des échanges confidentiels ; si on chiffre, donner à son correspondant les moyens de le déchiffrer (s'il s'agit d'une clé secrète de déchiffrement, il est évident qu'elle ne doit pas être transmise elle-même par courrier électronique) ;
- pour tout courrier important, configurer le logiciel de courrier pour demander un accusé de réception ; contacter le destinataire si l'accusé de réception n'arrive pas ;
- en cas de réception d'un courrier important (par exemple report de la date de remise des offres, modifications du DCE…) vérifier auprès de l'émetteur qui apparaît sur le courrier que c'est bien lui qui a émis ce courrier.

ANNEXE 14 : sécurité du personnel et sensibilisation - quelques conseils élémentaires

« La plupart des problèmes de sécurité ne sont pas dans l'ordinateur, ils sont dans ce qui est assis devant l'ordinateur »

Cette boutade n'est pas tout à fait exacte, car l'ordinateur et ses logiciels sont très imparfaits, et on y découvre continuellement des problèmes de sécurité. Des expériences ont même montré qu'il suffit de quelques minutes de connexion à internet pour compromettre un ordinateur non protégé, c'est à dire pour qu'il soit infecté par au moins un programme malveillant : virus, espiogiciel (spyware), cheval de Troie (qui peut le transformer en « zombie », c'est à dire en donner la maîtrise à l'attaquant), ver (par lequel il attaque lui-même d'autres ordinateurs) etc. A noter que cette compromission peut rester discrète, et n'avoir comme effet perceptible par l'utilisateur que quelques anomalies de fonctionnement apparemment banales.

Toutefois, il est bien certain qu'aucune protection ne tient si l'utilisateur du poste de travail est inconscient ou négligent ; un minimum de précautions de bon sens permettent d'éviter la plupart des malveillances et des accidents.

1. Protéger l'accès au poste de travail et au réseau

Utiliser des mots de passe forts et les changer régulièrement. Un mot de passe de cinq caractères peut être deviné en quelques secondes, un mot de passe qui figure dans un dictionnaire, même long, est également vulnérable (« attaques par dictionnaire »). Le mot de passe doit comporter au moins huit caractères, lettres, chiffres et caractères spéciaux (ponctuation, parenthèses etc.). Ce mot de passe doit être facile à mémoriser et si on l'écrit, parce qu'on craint de l'oublier, il doit être conservé en lieu sûr : il est aussi imprudent de l'écrire sur un « post-it » collé sous le clavier que de laisser la clé de son appartement sous le paillasson du palier. Enfin, il est prudent d'en confier une copie à une personne de confiance, dans une enveloppe scellée, pour qu'en l'absence du titulaire du poste les personnes autorisées puissent néanmoins y accéder en cas de besoin légitime.

Exemples :

- pour n'avoir pas protégé l'accès à son poste de travail, une personne a été accusée d'avoir envoyé des mails pornographiques. En fait, c'était une mauvaise plaisanterie d'un de ses collègues de bureau ;
- Une malveillance interne vient effacer des fichiers importants ; comme ils n'étaient pas sauvegardés (deuxième imprudence), un travail considérable est perdu ;
- De la même façon, des fichiers confidentiels sont compromis discrètement, et la victime ne s'en aperçoit que beaucoup plus tard, quand les dommages sont déjà importants.

2. Etre attentif aux pièces jointes aux courriers électroniques, et aux modules téléchargés depuis internet

Ce sont d'excellents moyens d'infection par des virus et autres programmes malicieux. Il ne faut donc pas :

- utiliser la fonction « prévisualisation » du contenu des courriers électroniques ;
- ouvrir la pièce jointe quand l'antivirus l'a signalée comme infectée ;
- ouvrir les courriers provenant d'inconnus ;
- ni ceux dont l'apparence est surprenante, même s'ils semblent provenir d'un expéditeur connu :
    - rédigés dans une langue étrangère, alors que le correspondant s'exprime en français ;

- objet peu compréhensible ;
- annonce d'un problème sur l'ordinateur, et conseils pour installer des « correctifs » ;
- annonce d'erreurs de facturation pour un service inconnu, ou inutilisé ;
- pièces jointes suspectes (extensions .exe, .scr, .pif etc.) ou sans rapport avec le texte du message.

Exemples : toutes les attaques de virus qui peuvent détruire les fichiers du poste de travail, paralyser le réseau auquel il est relié et qui nécessitent toujours un gros travail de désinfection et de réparation.

3. Installer et tenir à jour l'antivirus quotidiennement sur tous les postes de travail

Le délai entre la première apparition d'un virus et sa propagation mondiale s'est considérablement raccourci ; et on a vu les virus les plus virulents infecter en quelques heures une part importante des ordinateurs dans tous les pays. La mise à jour des antivirus doit donc être quotidienne, pour disposer toujours d'un produit capable de détecter les dernières attaques. Certains éditeurs proposent des mises à jour automatiques, chaque fois qu'ils modifient leur produit. Les utilisateurs doivent savoir comment réagir quand l'antivirus détecte un fichier infecté.

Se faire infecter par un virus n'est pas une fatalité ; envoyer un virus à ses correspondants est souvent un signe de négligence qui peut détruire l'image que l'on s'efforce de donner.

4. Disposer d'un pare-feu

5. Désinstaller les logiciels inutilisés et supprimer les comptes utilisateur périmés

Ce sont autant de possibilités d'attaque que l'on peut supprimer sans inconvénient. Nettoyer complètement les disques des ordinateurs réformés ou, mieux, les détruire : ces disques contiennent souvent des informations sensibles que l'on peut récupérer, même si les fichiers ont été supprimés des répertoires par logiciel ou si l'ordinateur est apparemment inutilisable.

Exemple : un magistrat utilisait son ordinateur personnel pour ses besoins professionnels ; cette machine est tombée en panne, et son propriétaire l'a jetée au bout de quelques années. Celui qui l'a récupérée, dans la poubelle, a pu retrouver les fichiers sensibles puisqu'ils étaient toujours présents sur le disque : il a prévenu la police et le magistrat a été réprimandé.

6. Contrôler l'accès physique aux ordinateurs.

Aussi élaborées que soient les protections logiques d'un ordinateur, elles peuvent être défaites si l'attaquant a accès physiquement à la machine. Si les contrôles d'accès logiques ont déjà été faits (machine déjà démarrée, déjà connectée au réseau par son utilisateur légitime), et que l'ordinateur est laissé sans surveillance, l'intrus n'a même plus besoin de les contourner ces protections logiques.
Protéger les données contre les accidents : sauvegardes des fichiers importants, éventuellement stockage de certaines sauvegardes sur un autre site etc.

7. Edicter des règles d'utilisation de l'informatique par les employés

Notamment :

- déconnexion ou au minimum verrouillage de l'économiseur d'écran avant de laisser l'ordinateur sans surveillance, même pour un bref instant ;
- rendre les employés responsables des ordinateurs portables qui leur sont confiés ;
- interdire l'utilisation personnelle et familiale de ces machines ;
- interdire l'utilisation d'ordinateurs personnels sur le réseau de l'entreprise ;
- règles d'utilisation d'internet (par exemple restrictions sur les sites accessibles, interdiction de participer aux forums depuis le poste professionnel…) ;

- responsabilité des employés en cas d'infraction aux règles.

8. Appliquer les mises à jour de sécurité des logiciels

Des vulnérabilités sont continuellement découvertes dans les logiciels du commerce et les éditeurs publient les correctifs nécessaires. On constate que des programmes exploitant ces vulnérabilités sont disponibles sur internet très rapidement après la publication de la vulnérabilité elle-même : il est donc indispensable que chaque utilisateur mette en place les correctifs dès qu'ils sont publiés[22].

Exemple : beaucoup de virus exploitent des vulnérabilités de produits très répandus. Dans bien des cas, ces virus ont eu des effets dévastateurs alors qu'ils n'auraient eu que des effets limités si les correctifs de sécurité avaient été appliqués (y compris, dans plusieurs cas d'ailleurs, par l'éditeur lui-même du logiciel erroné qui avait négligé de se protéger contre ses propres erreurs).

9. Mettre en place un système de contrôle d'accès au réseau

[22] L'installation de ces correctifs peut-être une opération lourde, si le parc d'ordinateurs concerné est important. De plus il est arrivé que certains correctifs soient incompatibles avec d'autres applications déjà installées sur les machines. Pour ces raisons, il est fréquent que les correctifs ne soient pas installés dès leur publication, mais seulement périodiquement, après s'être assuré qu'ils n'ont pas d'effet indésirable : les ordinateurs restent donc vulnérables pendant quelque temps, et il faut peser le risque encouru.

ANNEXE 15 : liste des membres du groupe de travail

Entité	Nom
AABS Ernst & Young	Thierry Jardin
Achatpublic.com	Dimitri Mouton
Achatpublic.com	Abdelmalek Benzenati
ADCS	François Hauser
Adésium	Yahya Barbara
Adésium	Valérie Guilbert
Alinitia	Christian Vormus
Assemblée des Chambres Françaises de Commerce et d'Industrie	Franck Olivier
Aud'system	Henri Hovette
Cofima Consulting	Jacques Cosquer
CAPEB	Didier Lefebvre
DoubleTrade	Alexandre Sidommo
Economie Numérique Conseil	Bruno Boutteau
e-marchéspublics.com	Régis Legros
Interbat Services	Casimir Decas
LexBox	Jacques Debiez
LexBox	Jean-Claude Escriva
LMSanté Group	Eric-Jean Desbois
Ministère de l'Education nationale, de l'Enseignement Supérieur et de la Recherche	Dominique Alglave
Ministère de la Défense - Délégation Générale pour l'Armement	Michel Cadic
Ministère de la Défense	Emmanuelle Plessiet
Ministère de l'Economie, des Finances et de l'Industrie Direction des Affaires Juridiques	Jean-Luc Genay
Ministère de l'Economie, des Finances et de l'Industrie Direction des Affaires Juridiques	Hervé Le Thierry
Ministère de l'Economie, des Finances et de l'Industrie Délégation aux Systèmes d'Information	Jean-Louis Ferracci

Entité	Nom
Ministère de l'Economie, des Finances et de l'Industrie Délégation aux Systèmes d'Information	Pierre Jean-Louis
Ministère de l'Economie, des Finances et de l'Industrie Direction du Personnel, de la Modernisation et de l'Administration Sous-direction de l'Immobilier	Pascal Frey
Ministère de l'Economie, des Finances et de l'Industrie Direction du Personnel, de la Modernisation et de l'Administration Sous-direction de l'Immobilier	Eric Doucet
Ministère de l'Economie, des Finances et de l'Industrie Direction du Personnel, de la Modernisation et de l'Administration Sous-direction de l'Informatique et des Nouvelles Technologies	Christophe Alviset
Ministère de l'Economie, des Finances et de l'Industrie Direction du Personnel, de la Modernisation et de l'Administration Sous-direction de l'Informatique et des Nouvelles Technologies	Roland Margueret
Ministère de l'Economie, des Finances et de l'Industrie Direction du Personnel, de la Modernisation et de l'Administration Sous-direction de l'Informatique et des Nouvelles Technologies	Emmanuel Mornet
Ministère de l'Economie, des Finances et de l'Industrie Direction Générale de l'Industrie, des Technologies de l'Information et des Postes	Daniel Depardieu
Ministère de l'Economie, des Finances et de l'Industrie Direction Générale des Douanes et des Droits Indirects	Aline Giannoni
Ministère de l'Economie, des Finances et de l'Industrie Direction Générale des Douanes et des Droits Indirects	Spitoni
Ministère de l'Economie, des Finances et de l'Industrie Haut Fonctionnaire de Défense	Jean-François Pacault
Ministère de l'Economie, des Finances et de l'Industrie Institut National de la Statistique et des Etudes Economiques	Hervé Boudier
Ministère de l'Economie, des Finances et de l'Industrie Mission pour l'Economie Numérique	Marc Lebreton
Ministère de l'Emploi, du Travail et de la Cohésion Sociale	Isabelle Desmettre
Ministère de l'Intérieur, de la Sécurité Intérieure et des Libertés Locales	Dominique Schlienger
Ministère de l'Intérieur, de la Sécurité Intérieure et des Libertés Locales	Akli Idir
Ministère des Affaires Etrangères Direction Générale de l'Administration	Marc Halteau
Ministère des Affaires Etrangères Direction Générale de l'Administration	Michel Pollez
M-SecureIT	Philippe Martraire
Omnikles	Jean-Christophe Didier

Entité	**Nom**
Services du Premier Ministre Direction des Services Administratifs et Financiers	Max Valems
Services du Premier Ministre Secrétariat Général de la Défense Nationale	Stanislas De Maupeou
SIS	Sylvain Ribout
Thales	Bernard Delecroix
Union des Groupements d'Achats Publics	Fu Kang Lee
Union des Groupements d'Achats Publics	Richard Savoldelli
Ville de Paris	Jean Benard