Agence de Mutualisation des Universités et Etablissements

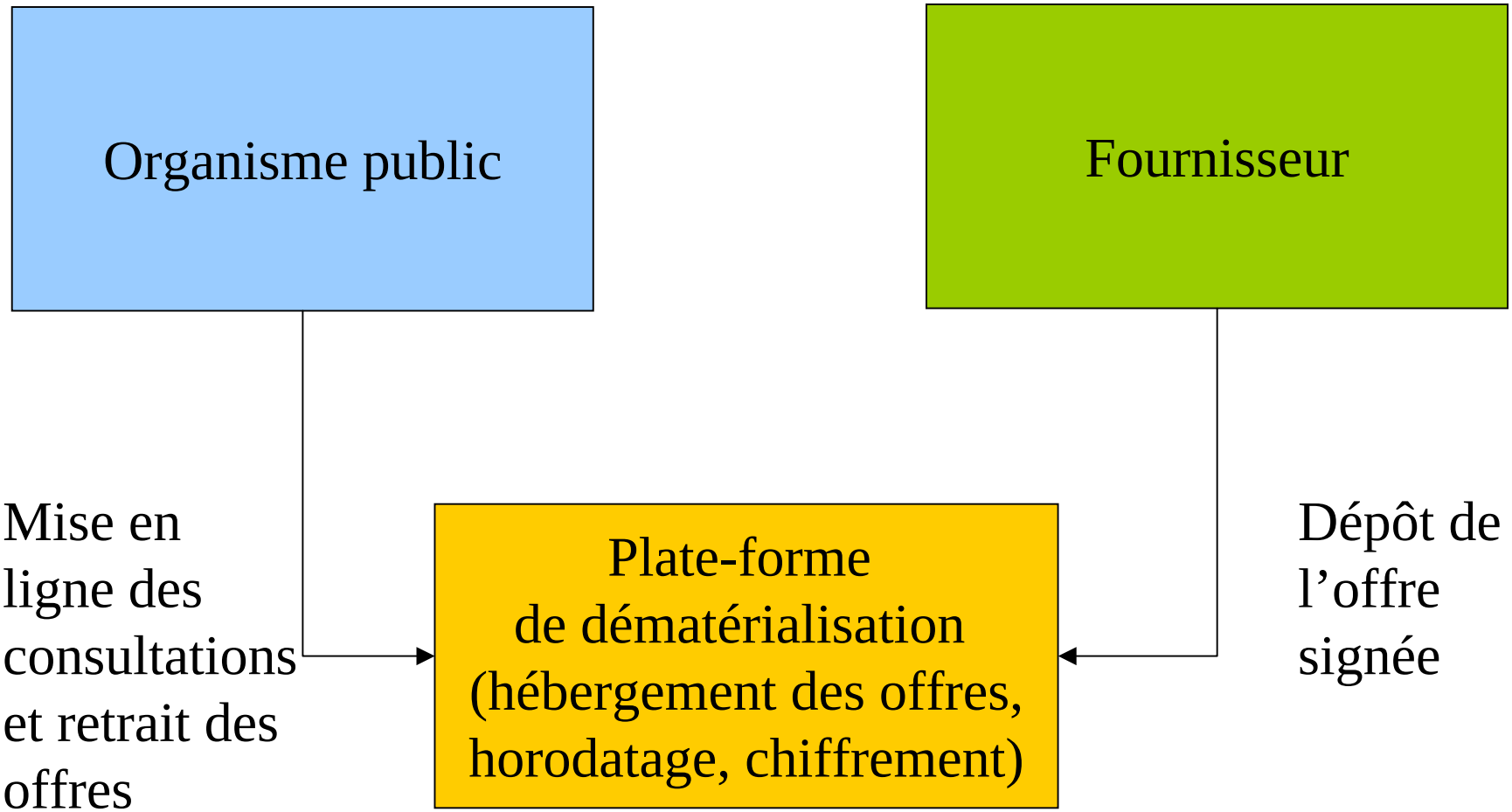
Eléments techniques de la confiance dans les procédures de dématérialisation des marchés

Serge Aumont / Florent Guilleux
CRU

Objet

- Les éléments techniques de sécurité dans la rédaction du cahier des charges de cet appel d'offres et dans l'évaluation des offres
- Des points que vous devez avoir à l'esprit pour utiliser la plateforme
- Attention particulière à tout ce qui pourrait remettre en cause la validité de la procédure
- Simplifier au maximum le processus

Schéma général de fonctionnement



Objectifs techniques

- Intégrité et non répudiation de l'appel d'offres
- Intégrité, imputabilité et non répudiation des offres
- Datation des offres
- Confidentialité et séquestre des offres
- Antivirus
- Journaux des procédures
- Disponibilité du service
- Archivage des offres

L’appel d’offres

- Les documents de l’appel d’offres ne sont pas obligatoirement signés par la personne publique. Le dossier d’appel d’offres papier existe toujours et peut servir de référence.
  - Pas de gros problème d’imputabilité ou d’intégrité
  - L’acheteur ne détient donc pas obligatoirement un certificat de signature

amue

Les offres

- Intégrité des enveloppes et de leur contenu
  - Signature de l'ensemble de l'enveloppe (par exemple .zip) pour se prémunir de la perte d'un élément.
  - Assurée par la signature de chaque document par le soumissionnaire

séminaire

Signature des offres

- La signature prouve l'intégrité et l'identité du soumissionnaire. Elle prouve l'engagement de l'auteur ("**lu et approuvé**").

- Elle doit être faite au moyen d'un certificat personnel du soumissionnaire reconnu par l'acheteur.

Signature des offres

- Quelles Autorités de Certification reconnaître pour cet usage ?
  - Politique de référencement du MINEFI
  - http://www.minefi.gouv.fr/dematerialisation_icp/dematerialisation_declar.htm
- La délivrance d'un certificat aux entreprises qui répondent fait-elle partie de la plateforme de dématérialisation ?
  - Non

Signature des offres

- Comment vérifier la signature “plus tard” ?
- La vérification de la validité d’un certificat doit vérifier la révocation
- (CRL ou OCSP)

Signature des offres

- La signature étant valide, comment s'assurer qu'elle est bien le fait d'une personne de l'entreprise ayant cette prérogative ?
  - Comment fait-on pour une procédure papier ?

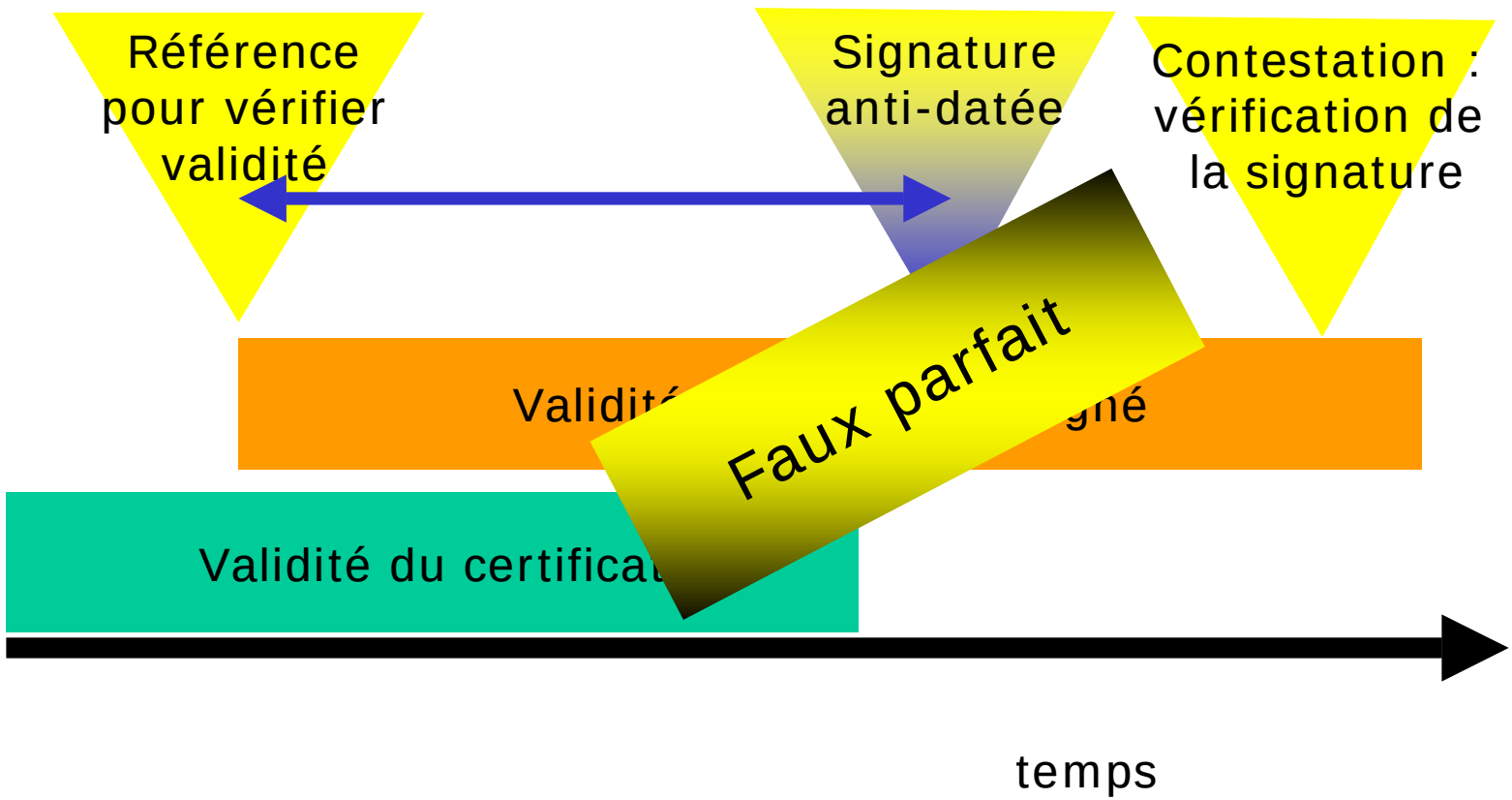
Signature des offres

- La plateforme doit intégrer un logiciel de signature et de vérification de signature
- On préférera l'intégration par une applet JAVA à l'installation d'un logiciel spécifique sur les postes clients de la plateforme
- Le format des documents est libre. Penser à imposer dans le règlement de consultation un format connu sur le poste de la PRM.
- "*what you see is what you sign*" : préférer pdf aux formats Microsoft

amue

séminaire

Pourquoi horodater les signatures ?



Horodatage

- La datation des différents documents et des différentes actions d'une procédure d'appel d'offres est importante.

- L'horodatage ne se limite pas à l'utilisation d'une horloge précise, il faut la rendre infalsifiable, c.à.d la marquer au moyen d'un jeton signé par une autorité d'horodatage.
  - Norme technique RFC 3161 respectée mais mise en oeuvre par l'opérateur de la plateforme

Pourquoi on peut se passer de l'horodatage

- L'horodatage est une montagne technique
- La réglementation n'est pas terminée dans ce domaine
- Les dates contenues dans les journaux de la plateforme sont suffisantes car elles ne sont fournies ni par l'acheteur, ni par le soumissionnaire.

Confidentialité

- Il faut assurer la confidentialité des offres
  - Le soumissionnaire chiffre son offre au moyen d'un "*bi-clef de chiffrement*" de l'acheteur
  - Seul le titulaire de ce bi-clef peut ouvrir les plis
- Disponibilité de ces bi-clef ?
  - L'opérateur de la plateforme doit délivrer ces bi-clés aux établissements.

Confidentialité

- Délégation de rôle au sein de l'établissement. La dématérialisation ne doit pas empêcher les chefs d'établissements de désigner une personne de leur choix pour l'ouverture des plis.
  - Le bi-clé n'est pas un certificat (il n'est pas personnel), il est de préférence sur un support cryptographique matériel

Confidentialité

- En cas de perte du bi-clef de chiffrement, une procédure doit permettre cependant d'accéder aux plis des marchés en cours.
  - Un service de recouvrement de la clé privée de chiffrement doit être disponible.

Antivirus

- Du fait du chiffrement des plis, l'opérateur de la plateforme ne peut accéder aux documents et ne peut y rechercher les virus.
  - Le poste client de l'acheteur doit être équipé d'un ou plusieurs antivirus. On procède à une mise à jour des signatures des virus juste avant l'ouverture des plis

Sequestre des offres

- Les plis ne doivent pas être ouverts avant une date déterminée.
  - La plateforme surchiffre les plis. Les plis sont réputés avoir été ouverts au moment où la plateforme délivre la clé de déchiffrement à l'acheteur. Les journaux de la plateforme apportent la preuve de cette date (cf horodatage).
  - Attention à ne pas télécharger par erreur la clé de chiffrement avant l'heure.

Journaux

- La plateforme assure l'intégrité des journaux
- Chaque évènement journalisé est signé par leur auteur (optionnel)
- Les journaux des différentes procédures d'un établissement sont accessibles à cet établissement (exclusivement)

Disponibilité

- L’indisponibilité de la plateforme peut empêcher la réunion d’ouverture des plis.
- Elle est susceptible d’être un argument pour contester la validité d’un marché (si un fournisseur ne peut déposer son offre).

- Obligation de disponibilité dans le cahier des charges.
- Les fournisseurs peuvent déposer la signature des documents 24h avant les documents eux-mêmes
- L’acheteur peut télécharger les documents avant d’avoir la clé pour les déchiffrer

amue

Archivage

- L’archivage des différentes pièces et des journaux est une fonction importante. La plateforme propose le téléchargement de l’ensemble de ces documents à des fins d’archivage.

- La plateforme archive elle même ces données (optionnel)
  - Les établissements doivent archiver eux-mêmes ces documents (le disque dur du PC n’est pas suffisant)

séminaire