ADULLACT

Association des Développeurs et des Utilisateurs de Logiciels Libres pour les Administrations et les Collectivités Territoriales

Réponse de l'ADULLACT à l'appel à commentaires de l'ADAE « Protocole d'échanges pour l'administration électronique » v2.0

13/09/05

Table des matières

1 - Remarques Générales....1

2 - Comparatif technique....6

Analyse du tableau comparatif....6

Remarques connexes....7

3 - Questions de la section 3 « Enjeux et besoins » :....8

Données transportées....8

Transport et connectivité....9

Sécurité....10

Qualité de service....12

Orchestration de service....13

Routage....14

4 - Questions et texte de la section 4 « Description du protocole »....14

Format des données....15

Protocole....15

Architecture d'échange des messages....16

Gestion de la sécurité....18

5 - Questions de la section 5 « Hub d'échanges » :....19

6 - Robustesse et performances....20

7 - Conclusion....21

ADULLACT

Association des Développeurs et des Utilisateurs de Logiciels Libres pour les Administrations et les Collectivités Territoriales

0 Remarques Générales

Le document proposé par l'ADAE sous la forme d'un appel à commentaires est au cœur des problématiques posées par la mise en œuvre de la e-administration et préfigure (d'une certaine façon) un modèle de fonctionnement de l'administration française pour de nombreuses années futures. C'est pourquoi les collectivités locales ne peuvent rester en retrait dans ce débat, elles sont en effet un des maillons essentiels de l'administration française, notamment dans leurs compétences propres et dans celles qu'elles exercent pour de nombreux organismes, au premier rang desquels on trouve l'état.

L'appel à commentaires en question est purement technique alors que la réflexion sur les modes opératoires régissant la télétransmission de contenus ne peut s'aborder et se résoudre à partir d'une seule approche technique ou techniciste et ce pour deux raisons :

- ✔ Nécessité de prendre en compte une des spécificités de l'administration française : les collectivités territoriales s'administrent librement et ne sont pas des succursales d'un système centralisé (la décentralisation est non seulement un argument de transfert de charges mais une réalité politique et organisationnelle),

- ✔ La mutation vers la e-administration sera longue et si l'on s'imagine qu'elle sera facile, on se trompe lourdement. Le poids des contraintes notamment culturelles, mais aussi la réalité économique, la diversité des situations sont autant de freins à son déploiement. C'est pourquoi nous préconisons la proximité avec les cultures "papier" d'aujourd'hui, condition d'appropriation de ces nouveaux modes.

Un autre élément essentiel est absent de la réflexion proposé : la cible des usagers, des citoyens. Comment peut-on aujourd'hui imaginer un système relationnel entre administrations sans intégrer les usagers qui sont la finalité de l'administration elle-même et qui seront dotés prochainement (projet CNIE) d'une signature électronique.

Enfin, les modes de travail des collectivités, avec d'une part les services de "production" et les nécessaires et réglementaires validations par les élus impliquent un mode d'approche particulier et des outils spécifiques.

ADULLACT

Association des Développeurs et des Utilisateurs de Logiciels Libres pour les Administrations et les Collectivités Territoriales

Des années de travail, d'expérimentation, une claire conscience des possibilités financières des collectivités, des milliers de contacts avec les responsables (cadres et élus) de ces collectivités, de toute nature et de toute taille nous ont amené à proposer une vision que nous rappellerons en introduction au commentaire du document de l'ADAE.

Le parti pris de cette réponse repose sur deux principes :

- ✔ Ne pas demander plus à l'électronique qu'aux procédures papier,
- ✔ Garantir la qualité de l'échange de flux de données, ces flux étant émis par des acteurs indépendants, autonomes et responsables.

Quelques remarques sur l'introduction et la mise en contexte du document :

- Concernant le protocole à choisir le texte dit : *« **Ce protocole devra fournir un certain nombre de fonctionnalités, énumérées dans la suite de ce document, tout en respectant les normes et standards actuels et en devenir, de manière à assurer sa pérennité et son interopérabilité. »***

  On devrait donc trivialement rejeter tout choix de protocole propriétaire et donc, de facto, le protocole de FAST.

- La mise en contexte du document précise, concernant l'architecture à choisir, que : ***« Elle doit aussi servir de base aux communications avec les partenaires européens voire être ouvert à d'autres partenaires extra-nationaux. »***

  Cette exigence offre un nouvel argument pour rejeter FAST car cette solution franco-française poserait problème dans le cadre de l'européanisation prévisible de l'administration électronique.

- Notons que la norme eLink, bien que proche de ebMS2, est toutefois propriétaire. Le texte dit : « ***Il a donc paru plus opératoire de présenter en restant factuel, une comparaison des fonctionnalités par besoin en s'appuyant sur le protocole européen eLink en cours de validation.*** »

  Cette vision privilégie un standard propriétaire qui a délibérément fait abstraction de l'existence de la Recommandation de standardisation ISO 15 000 – 2. Les comparaisons faites sont donc de facto biaisées. Nous récusons ce parti pris.

- Le texte dit de ACTES et Hélios : « ***Ces deux projets s'appuient sur le protocole d'échanges FAST développé par la CDC.*** »

  Dès le départ la problématique est mal posée car elle repose sur des affirmations orientées. Le deuxième alinéa "à titre d'exemple" affirme deux constats faux :

  - ✔ le projet Hélios ne s'appuie pas sur le protocole d'échanges FAST, mais sur des protocoles de la famille PES et la DGCP accepte tous les modes de communication avec ses serveurs (comme elle le fait d'ailleurs aujourd'hui avec les autres protocoles, que ce soit sous la forme de liaisons directes, de l'utilisation de TEDECO ou d'envois postaux de supports électroniques). Les responsables du projet Hélios ont inscrit cette liberté de choix des modes de communication dans les principes fondateurs de la charte nationale signée par toutes les associations d'élus,

  - ✔ le projet ACTES du ministère de l'intérieur propose aux collectivités trois modes de relation entre la "sphère des collectivités" et la "sphère du ministère", l'un de ceux-ci étant la relation directe entre les acteurs selon un cahier des charges qui vient d'être publié et qui n'est pas le protocole privatif FAST.

- ***« ebMS2 : ce protocole utilisé dans le cadre d'échanges ebXML (electronic business XML) a été élaboré sous l'égide du consortium OASIS (Organization for the Advancement of Structured Information Standards). La version 3, en gestation, devrait se rapprocher des standards émergeants liés aux services Web. »***

  Cette dernière phrase, que nous jugeons tendancieuse, laisserait à penser qu'ebMS2 a encore besoin d'être perfectionné. Nous récusons ce parti pris dans la mesure où ebMS2 est déjà largement exploité en production avec succès en milieu industriel.

Il est d'ailleurs intéressant de noter que la "relation directe", qu'elle concerne Hélios ou Actes, démontre à l'évidence que les systèmes d'information récepteurs des ministères sont en situation de recevoir et donc de contrôler les données envoyées, ce qui rend toute fonction de contrôle de la structure des données inutile au niveau du Tiers de Télétransmission (TdT). Nous y reviendrons. Il est clair que les acteurs de la e-administration échangent des flux de données variés, flux organisés selon des schémas ou des formes qui conviennent aux dits acteurs (qui ne sont donc pas nécessairement publiques), schémas qui doivent être des normes dans le cas d'échanges s'inscrivant dans des procédures réglementaires. Quant aux contraintes de sécurité importantes… la principale (et la seule ?) est que le courrier arrive à son destinataire sans avoir été modifié, les données quant à elles étant dans 99 % des cas publiques, leur confidentialité est toute relative…

Par ailleurs, concernant l'introduction de la notions de « hubs », il ne faut pas faire un sondage très profond dans le milieu des collectivités territoriales pour se rendre compte que ce mode d'organisation basé sur la notion de « hubs » plus ou moins obligatoires n'est pas concevable dans les années qui viennent. Une telle vision est à contre culture de tous les responsables de collectivités.

ADULLACT
Association des Développeurs et des Utilisateurs de Logiciels Libres pour les Administrations et les Collectivités Territoriales

1 Comparatif technique

Analyse du tableau comparatif

« 3.1 Format des données » : FAST encode tout dans le document XML alors que eLink comme ebMS2 permettent l'attachement de fichiers (SWA : SOAP with attachments) pour placer des binaires en pièces jointes. On imagine bien que cette fonctionnalité serait bénéfique pour associer des données telles que des photos, sons ou tout autre type de document. Notons que ceci constitue un plus et que l'encodage des documents en XML reste possible avec ebMS2 et eLink.

« 3.2.1 Protocole de transport » : FAST ne permet que de transmettre sur HTTP(S) alors que les autres solutions offrent, en plus, un support pour MOM ouvrant ainsi des perspectives en terme d'évolutivité et d'adaptativité.

« 3.2.2 Routage » : FAST ne permet que le P2P alors que les autres solutions offrent, en plus, le mode Publish/Subscribe, le mode Request/Response et la notion de noeuds intermédiaires (routage multiple). Par ailleurs, ebMS2 permet également le masquage les intermédiaires offrant ainsi de nouvelles garanties en terme de confidentialité.

« 3.2.3 Messages de service » : Concernant ce point, eLink pêche par limitation de ses possibilités. FAST offre, en plus, la récupération d'information sur le transport. Par contre, c'est ebMS2 qui est de loin le plus complet sur ce point. En effet, il permet tout ce que FAST permet ainsi que le ping de service. Cet outil pourrait être exploité afin d'optimiser les connexions au travers d'outils de QoS (Quality of Service).

« 3.2.4 Corrélation » : La solution FAST se limite à la définition de liens entre messages. eLink se limite à la possibilité d'identifier les applications d'envoi et de connexion et de découper les messages de grande taille. Une fois encore, ebMS2 emporte la palme en associant aux messages identifiant de message et identifiant de corrélation tout en permettant d'ordonnancer les messages.

« 3.3.2 Signature » : Sur ce point, eLink et ebMS2 se contentent l'utilisation de XML Signature alors que FAST exploite XAdES (extension de XML Signature avec archivage à long terme) en natif. On peut toutefois utiliser XadES dans ebMS2 en exploitant l'API ad hoc. Quel que soit le futur protocole retenu, il est par ailleurs recommandé d'utiliser des outils de vérification et gestion des preuves capables de gérer en natif les différents standards de signature et leurs évolutions dans le cadre des échanges électroniques.

Remarques connexes

- La mise en contexte du document précise, concernant l'architecture à choisir, que : ***« Elle doit aussi servir de base aux communications avec les partenaires européens, voire être ouverte à d'autres partenaires extra-nationaux.»***

  Nous adhérons avec cette vision des choses et pensons que, dans le cadre de l'européanisation prévisible de l'administration électronique, les choix retenus doivent prendre en compte la reconnaissance internationale des standards. Nous prenons pour référence, en raison de sa reconnaissance par le tissu industriel international et des garanties qu'elle offre en terme d'interopérabilité, la recommandation W3C ISO 15000-2.

Nous souhaiterions également qu'il soit possible d'attacher des fichiers en tant que pièces jointes. En effet, cette fonctionnalité nous parait très utile pour les documents qu'il est préférable de laisser sous forme binaire afin de ne pas perdre inutilement de la place et du temps de calcul dûs à des conversions multiples vers et à partir de BASE64 (comme le fait FAST par exemple). Nous préconisons donc un choix permettant à la fois l'empaquetage de documents en XML (pour joindre les documents textuels par exemple) et l'attachement de pièces jointes sous forme binaire.

Concernant le transport et le routage, nous préconisons que le maximum de protocoles restent autorisés. Par exemple, il doit être possible de transmettre sur différents protocoles (HTTP(S), (S)FTP, SSH...) et la possibilité de communiquer de manière asynchrone au travers d'un MOM doit être garantie afin d'éviter les engorgements et d'assurer la possibilité de découpler les applicatifs et les serveurs. Cette fonctionnalité permettrait d'ailleurs de répondre à un des besoins bien identifié dans l'appel à commentaires : ***« La plate-forme cible DOIT être apte à supporter la charge des mouvements de documents échangés dans le cadre des projets ADELE. Elle DOIT proposer des mécanismes de répartition de charge et de reprise sur incident. »***. En effet, l'utilisation de communications asynchrones va dans ce sens. Par ailleurs, nous préconisons que, en plus du mode *Request/Response*, le mode *Publish/Subscribe* puisse être exploité. Ce dernier pouvant être particulièrement pertinent dans le cadre de la relation avec les citoyens.

On notera que la solution FAST avance la notion de « preuves électroniques » comme justification de son existence, alors que les autres protocoles standard déjà existants intègrent déjà ce genre de « preuves ». D'autant plus que, en complément du protocole utilisé (par exemple ebMS2), il est possible d'intégrer des outils de vérification et gestion de preuves avancées dans le cadre d'un portail TdT.

ADULLACT

Association des Développeurs et des Utilisateurs de Logiciels Libres pour les Administrations et les Collectivités Territoriales

2 Questions de la section 3 « *Enjeux et besoins* » :

Données transportées

Ref	Question	Commentaire
1.1	Avez-vous un besoin fort concernant l'acheminement de pièces jointes binaires ? De quel type (PDF, RTF, GIF, JPEG, etc) ?	Le besoin en pièces jointes (qu'elles soient jointes ou encapsulées) est important pour les procédures comptables et les procédures techniques (urbanisme, marchés publics, action sociale…). Ces pièces sont aujourd'hui de tous types, actuels et futurs, mais sont appelées à tendre vers des formats utilisables (notamment XML comme les factures dans Hélios). Pour ce qui concerne les textes et les données, le format XML doit être le format recommandé.
1.2	Quelle est la taille de vos plus volumineux messages (pièces jointes comprises) ?	Un marché, un permis de construire, un PLU peuvent représenter des centaines de Mo.
1.3	Pensez-vous qu'il puisse être utile de vérifier la structure des données transportées ?	Non. Aucun système d'information n'importe des données sans en vérifier la structure. Ce serait donc un doublon inutile au niveau de la transaction. Cela pourrait être une violation de la confidentialité de la correspondance
1.4	Pensez-vous qu'il soit utile de pouvoir vérifier les signatures électroniques apposées sur les données transportées ?	Il faut faire une différence entre les signatures des données transportées et les signatures des acteurs de la procédure (expéditeur et destinataire) qui, elles seules doivent être "valides", donc contrôlées sur les listes de révocation on line des opérateurs de certification. Les enveloppes n'étant pas ouvertes, les signatures des données ou des documents ne sont pas contrôlées
1.5	La possibilité de détecter les doublons vous semble-t-elle utile ? Si oui, comment les identifier, suivant quels critères ?	Non. Chaque expéditeur est maître de ses envois et on ne « lit » pas les données.

Ces questions orientent l'appel à commentaires vers une solution qui serait institutionnelle, d'une certaine façon obligatoire. Au nom de quels textes de référence pour ce qui concerne les collectivités, au nom de quelle logique économique de libre choix et de concurrence.

Transport et connectivité

Ref	Question	Commentaire
2.1	Vous semble-t-il nécessaire de pouvoir diffuser un message vers plusieurs destinataires ? Si oui, qui doit avoir la liste des destinataires : l'émetteur ou le hub d'échange ?	Oui. C'est l'émetteur qui maîtrise ses listes, soit directement, soit à partir d'un annuaire national.
2.2	Disposez-vous d'un hub d'échanges ou d'une plateforme B2B ? Utilise-t-il un format d'échanges particulier ?	Non, ce qui n'est pas contradictoire avec la possibilité pour certaines catégories d'émetteurs de s'organiser dans des sphères "métiers", sphères alors positionnées comme des émetteurs normaux.
2.3	Quels sont les protocoles de transport et de connectivité que vous utilisez le plus (FTP, NFS, http, SMTP, JMS, interface propriétaire, etc.) ?	Tous!
2.4	Quelles sont les technologies que vous utilisez le plus (J2EE, .NET, Web services, interface propriétaire, etc.) ?	Toutes. Un protocole doit être indépendant de la technologie

L'utilisation de listes de diffusion (et d'accusés de réception par destinataire) sera un des "gains de productivité" essentiels de la e-administration. C'est une des raisons pour lesquelles le protocole d'échange sera beaucoup plus utilisé que, dans le modèle papier, la procédure LR avec AR.

Sécurité

Ref	Question	Commentaire
3.1	Authentification de l'application : faut-il s'assurer que le flux d'information provient bien d'une application donnée ?	Non. Le flux d'information est placé sous la responsabilité de son auteur. Le protocole n'intervient pas, ni sur son contenu, son origine ou sa structure.
3.2	Authentification de l'utilisateur : faut-il s'assurer de l'identité de l'utilisateur final émetteur du flux d'information ?	Il faut s'assurer de l'identité de l'émetteur. Pour une collectivité, ce sera la plupart du temps les responsables "courrier départ". Cette identité n'a, le plus souvent, rien à voir avec celle du ou des signataires des contenus… sauf si le maire ou le président font tout, tout seuls. Cf 1.4.
3.3	Le protocole d'échange véhiculera les informations nécessaires à la signature des messages, mais pensez-vous qu'il soit utile de gérer les signatures multiples sur un même document, sur des parties de documents, sur certaines pièces jointes ?	Il faut séparer la signature de l'envoi qu'assure le protocole, de la signature des pièces et données contenues dans l'envoi. **Le protocole n'a pas à connaître des contenus.** Le besoin de signatures multiples est un besoin réel, mais à l'intérieur des systèmes d'information (applications métiers) des acteurs, par exemple pour la signature du procès-verbal du conseil municipal (futur document électronique qui ne sort pas de la mairie (qui n'utilise donc pas le protocole).
3.4	Le protocole doit-il prévoir des informations de non-répudiation, c'est à dire de traces électroniques à valeur probante (signature de l'émetteur, du récepteur, d'un tiers de confiance et horodatage des messages) ?	C'est la fonction de la signature électronique.

3.5	Le protocole doit-il prévoir les informations nécessaires à l'archivage sécurisé des données échangées ?	Non. L'archivage électronique est un métier en lui-même, il ne doit pas être confondu avec la fonction de transmission et d'échange. Il sera assuré soit par le responsable lui-même (souvent l'émetteur), soit par un prestataire spécialisé. Nous préconisons l'ajout systématique à tout envoi vers un TdT d'une adresse d'archivage par défaut (adresse qui peut être interne). **L'archivage de la trace** de l'échange (sans son contenu) est lui absolument nécessaire. C'est la fonction de base du TdT.

Qualité de service

Ref	Question	Commentaire
4.1	Quelle est la fréquence attendue ?	S'il s'agit de la fréquence des envois, le déploiement de la e-administration, notamment si elle englobe comme nous le souhaitons la cible des usagers, aboutira à une fréquence importante. En annexe 2 figure une estimation de la montée en charge des procédures électroniques pour lesquelles l'usage d'un TdT semble utile.
4.2	La gestion des priorités pour acheminer des messages urgents vous semble-t-elle nécessaire ?	Non.
4.3	Les émetteurs doivent-ils pouvoir demander qu'un accusé de réception leur soit envoyé lorsqu'un message est remis au destinataire final ?	Oui. C'est une fonction de base. Cela suppose que soit généré un identifiant (par destinataire dans le cas d'un envoi à des destinataires multiples) lors de l'envoi afin que l'AR soit rapproché (de façon automatique dans l'application émettrice) avec l'envoi. Utilité du e-parapheur chez les acteurs des échanges.

De plus, au niveau messagerie, les plates-formes pourraient renvoyer automatiquement un message qui n'a pas été bien reçu, de sorte que des pertes de connexion temporaires demeureraient invisibles à l'application. Ce mécanisme de Reliability est inclus dans ebMS2.

Ref	Question	Commentaire
4.4	Les émetteurs doivent-ils pouvoir questionner des alertes spécifiques telles qu'une alerte en cas de non réception d'un accusé de réception dans des délais paramétrables ?	Il est souhaitable que le TdT informe les émetteurs de la non distribution du courrier à des fréquences qui pourraient être fixes (une semaine, deux semaines, un mois), et émettent des rappels automatiques vers les destinataires. Au-delà le courrier non distribué devrait faire l'objet d'une alerte définitive de non distribution et dégager la responsabilité du TdT.
4.5	Les émetteurs doivent-ils être notifiés dans le cas ou une anomalie surviendrait au cours d'un échange (signature invalide, destinataire injoignable, etc.) ?	L'interrogation des listes de révocation des opérateurs de certification producteurs des signatures électroniques de l'échange doit générer des alertes : refus de la transaction s'il d'agit de l'émetteur, procédure supra (4.4) avec commentaire (nature de l'anomalie).

Le système transactionnel fait apparaître clairement le besoin d'outils de gestion du courrier dans chacun des systèmes d'information (émetteur et destinataire), systèmes qui, pendant de nombreuses années, devront être cohérents avec les systèmes de gestion du courrier papier. C'est pourquoi ils se trouvent dans les systèmes d'information et non ailleurs.

Orchestration de service

Ref	Question	Commentaire
5.1	Les messages doivent-ils pouvoir être pilotés par un processeur ou un workflow ? En d'autres termes, un message doit-il pouvoir stocker des informations sur son état d'avancement, générer des messages informatifs de suivi ou encore être corrélé avec d'autres messages ?	Non. Voir point 4.4.

Il nous paraît utile de préciser quelques concepts de base.

L'enveloppe de transport

C'est une enveloppe numérique inviolable. Elle fonctionne comme une enveloppe papier classique : l'utilisateur, depuis son logiciel, insère des documents dans l'enveloppe numérique, écrit l'adresse du destinataire et la scelle. Pour effectuer cette dernière opération, un serveur externe demande à l'utilisateur de s'identifier (TdT).

Cela est possible à l'aide d'un certificat numérique qui va donner une valeur juridique à l'envoi.

Proposition de contenu de l'enveloppe :

- La référence interne de l'envoi attribuée par l'émetteur
- Le certificat X509 V3
- Le ou les destinataires
- L'intitulé (l'objet) de l'envoi
- L'objet complémentaire (facultatif)
- Le contenu de l'envoi (« enveloppes métier » ou données structurées ou documents)

S'il existe une liste de destinataires, chaque destinataire ne voit que son adresse.

Contenu d'un certificat

Le certificat contient un certain nombre de champs obligatoires et des extensions dont certaines sont facultatives.

Les champs obligatoires :

- Version : indique à quelle version de X509 correspond ce certificat
- Numéro de série : Numéro de série du certificat
- Algorithme de signature: identifiant du type de signature utilisée
- Emetteur : Distinguished Name (DN) de l'AC qui a émis ce certificat
- Valide à partir de: la date de début de validité de certificat
- Valide jusqu'à : la date de fin de validité de certificat
- Objet: Distinguished Name (DN) du détenteur de la clef publique
- Clé publique : infos sur la clef publique de ce certificat
- Signature : Signature numérique de l'AC sur l'ensemble des champs précédents

L'AC est l'opérateur de certification qui gère techniquement la vie du certificat. L'établissement du certificat dépend d'une AE qui peut être distincte de l'AC et relayée localement par des ALE (autorités locales d'enregistrement).

B - Les champs complémentaires :

Il est souhaitable de disposer d'informations complémentaires, clairement authentifiées, sur :

- le type du certificat : PM ou PP
- l'AE (autorité d'enregistrement),
- éventuellement l'ALE (autorité locale d'enregistrement).

Routage

Ref	Question	Commentaire
6.1	Quelles informations doivent être véhiculées par le routage pour permettre au document d'être routé vers le bon service et le bon traitement ? Quelles sont les informations qui vous sont nécessaires pour déterminer le destinataire de vos messages ?	Il suffit de l'identifiant électronique final du destinataire.

3 Questions et texte de la section 4 « *Description du protocole* »

- Cette section est introduite par : « ***Le protocole d'échanges eLink est donc le protocole retenu comme étant le plus représentatif des besoins pour les échanges du programme ADELE.*** »

  Pourquoi consulter si ce protocole propriétaire est considéré, a priori, comme étant le plus représentatif ? Aucun protocole étudié ne devrait être considéré comme « le plus représentatif ». Par contre, une norme reconnue internationalement telle que la recommandation ISO 15 000 – 2 peut être considérée comme la plus représentative du fait de son statut de standard ouvert développé dans le cadre des instances de standardisation de jure.

Format des données

eLink et ebMS2 sont considérés comme identiques sur ce point et critiqués pour le mélange XML/SWA qui, contrairement à ce qui est avancé, ne pose pas de problème pour la signature et l'encryptage des documents. FAST encode tout en base 64, plus volumineux. Notons que rien n'empêche de faire cela dans eLink ou ebMS2. (cf. commentaire de ***« 3.1 Format des données »***)

- Par ailleurs, concernant eLink, le texte dit : ***« XML n'est pas le format unique, l'utilisation exclusive d'outils de sécurité XML (Signature et Encryption) n'est pas possible .»***

Cette affirmation est erronée car XML Signature et XML Encryption traitent aussi bien les enveloppes MIME que les attachements SOAP qu'elles contiennent. XML Signature est la norme pour la signature. La spécification Web Services Security Core Specification d'OASIS décrit une méthode précise d'utilisation de XML Signature et Encryption pour SOAP (qui sera suivie par ebMS3).

- Au sujet de ebMS2, il est dit : « ***Un message ebXML, défini par la norme ebMS2, est constitué d'une enveloppe de message composée de plusieurs attachements MIME. De même que eLink, cette enveloppe est structurée en accord avec la spécification de SWA (SOAP With Attachement). »***

Il convient de rappeler que eLink et ebMS2 ajoutent une sécurité : une fois signé, il est impossible de substituer, d'ajouter ou retrancher des parties MIME. Celles-ci peuvent donc être sécurisées indépendamment une par une (exemple : certains documents sont déjà encryptés par l'application).

- Concernant MTOM, le texte dit : ***« Les technologies MTOM (Message Transmission Optimisation Mecanism) et XOP (Xmlbinary Optimised Package) sont sensées clore le débat en combinant les différentes techniques. Ces technologies sont des recommandations W3C et poussées par les principaux éditeurs. Le principe est d'encoder les données binaires dans le document XML sous la forme de données base64 qui permet de bénéficier des normes XML de sécurité et de Signature, et de laisser à l'implémentation l'extraction de ces données et leur placement en pièce jointe. Cette technologie serait parfaitement adaptée au transport d'un protocole tel que FAST : l'augmentation de taille liée à l'encodage serait résolue. Cependant, MTOM ne semble pas une solution assez mature à ce jour mais pourrait se présenter comme un compromis idéal entre les deux approches vues précédemment. Le protocole devra donc prévoir une évolution vers la technologie MTOM. A ce titre, on peut citer le cas de FAST car MTOM est compatible avec les options prises par FAST. Les impacts d'une migration sur l'existant seraient donc extrêmement limités. »***

Ces remarques sont valables pour tous les protocoles.

Protocole

Ref	Question	Commentaire
7.1	Que préconisez-vous : SWA ou MTOM (ou autre comme, par exemple, WS-Attachements/DIME) ?	A l'heure actuelle, SWA est la meilleure solution. Quid du futur ?
7.2	Voyez-vous d'autres limitations à l'utilisation de SWA comme mécanisme d'échange des pièces jointes ?	NON
7.3	La technologie MTOM vous paraît-elle une solution envisageable ? A quelle échéance ?	Oui. Qui le sait ?
7.4	Quel principe de double enveloppe préconisez-vous parmi ceux proposées ?	SWA cf. 7.1
7.5	Quelles informations doivent être véhiculées par le routage pour permettre au document d'être routé vers le bon service et le bon traitement ?	Voir réponse 6.1

Il est un peu tôt pour répondre à ces questions. Cette dynamique semble néanmoins incontournable dans un futur proche.

7.6	Quel est selon vous le calendrier réaliste que l'on peut attendre pour une implémentation opérationnelle de ces standards ?	De nombreuses applications envisagent l'utilisation de ces technologies dans des délais difficiles à préciser aujourd'hui
7.7	Faut-il aller vers ces standards (aujourd'hui pas matures et demain…) ?	Oui pour des raisons d'intéropérabilité et de standardisation

Architecture d'échange des messages

- Concernant le protocole de transport, le texte défend les concurrents de FAST car ce dernier ne propose rien dans le contexte des MOM et ne permet donc pas de communications asynchrones. Citons : « ***L'utilisation du mode asynchrone permet de découpler émetteur et récepteur. Le middleware de messages assure de plus une qualité de service avec la persistance des messages qui transitent et (selon le produit retenu) une durée de vie, le support du mode transactionnel (XA), la reprise sur incident, etc. Le principal inconvénient est l'absence de standard (à l'exception de JMS qui est standard au sein du monde J2EE mais n'a pas d'équivalent par ailleurs). »***

Ref	Question	Commentaire
7.8	Le support d'autres transports (SMTP, FTP, SFTP, SSH, etc.) vous paraît-il important dans le cadre des échanges entre organisations concernées par le programme ADELE ?	Oui pour répondre à des besoins ultérieurs ou pour répondre à des choix de sécurité ou de performances de certains utilisateurs

- Citons : « ***Les protocoles eLink, FAST et ebMS2 supportent le mode « point à point 1 1 ». eLink et ebMS2 supportent de plus le mode « publication/abonnement ». »***

  Bien que, a priori, seul le P2P semble nécessaire, notons que cette faiblesse de FAST peut poser des problèmes a posteriori car le mode publish/subscribe peut d'avérer très utile dans le cadre de la relation citoyen (Par exemple, dans le cadre de ACTES car les délibérations sont accessibles au public).

Ref	Question	Commentaire
7.9	Qui selon vous doit gérer les identifiants uniques : la plateforme d'échanges ou l'application émettrice ?	C'est la plateforme d'échange qui gère l'identifiant unique de chaque transaction

- On trouve en préliminaire aux questions 7.10 et 7.11 : *« **La définition du protocole aura pour base les messages de services proposés par eLink. Elle devra être suffisamment simple et extensible. »***

Ref	Question	Commentaire
7.10	La liste des erreurs vous paraît-elle suffisante dans le cadre des échanges des projets du programme ADELE ?	Oui
7.11	Quelles possibilités de suivi de message (cf FAST ; notifications d'avancement, positionnement d'alertes) vous semblent-elles pertinentes ?	Voir 4.4

Gestion de la sécurité

- Concernant le chiffrement, le texte dit : « ***Les protocoles évalués proposent un chiffrement des données XML assuré par le standard XML-Encryption. Le protocole eLink ne traite pas clairement le cas du chiffrement des données binaires jointes au message. La possibilité de chiffrer ces éléments est importante. De même la possibilité de chiffrer par partie semble intéressante. Le protocole FAST permet ce type de chiffrement partiel.*** »

Ref	Question	Commentaire
7.12	Quel mécanisme de chiffrement des documents joints serait-il préférable d'utiliser ?	Pas de chiffrement pour l'essentiel des procédures qui sont publiques. Ce n'est par ailleurs pas le protocole de télétransmission qui assure éventuellement cette fonction
7.13	Quel mécanisme de signature des documents joints serait-il préférable d'utiliser ?	Le protocole n'a rien à voir avec la signature des documents joints ou des données binaires
7.14	La technologie de signature XAdES est-elle, selon vous, pérenne et surtout utilisable sans contrainte ?	Oui. D'autres technologies (notamment XML signature - DSIG) sont utilisables pour signer une transaction.
	XAdES et XML DSIG sont tous les deux des standards reconnus en matière de signature électronique. XADES met en œuvre des niveaux de signature plus avancés et présente en contrepartie des contraintes d'implémentation plus importantes. Ces standards sont de toutes les façons destinés à évoluer (et pourquoi pas vers une réunification?). En l'absence d'indicateurs d'évolution fiables, les outils de vérification et de gestion de preuves électroniques se doivent de gérer ces deux standards de signature. XAdES et XML DSIG sont tous les deux des standards reconnus en matière de signature électronique. XADES met en œuvre des niveaux de signature plus avancés et présente en contrepartie des contraintes d'implémentation plus importantes. Ces standards sont de toutes les façons destinés à évoluer (et pourquoi pas vers une réunification ?). En l'absence d'indicateurs d'évolution fiables, les outils de vérification et de gestion de preuves électroniques se doivent de gérer ces deux standards de signature.	

4 Questions de la section 5 « *Hub d'échanges* » :

- Citons : ***« Le hub d'échanges DEVRAIT disposer d'un ensemble de connecteurs techniques permettant l'intégration des différentes organisations. Parmi les connecteurs techniques, on peut citer HTTP(S), Web Services (SOAP sur HTTP ou MOM), les principaux MOM du marché, .NET, Java, JMS, base de donnée (JDBC, ODBC), fichiers (NFS, FAT32, etc.)... »***

Ref	Question	Commentaire
8.1	Quels sont selon vous les connecteurs techniques indispensables ?	Hors protocole.

- Citons : ***« La passerelle DOIT assurer la compatibilité entre le deux formats en s'appuyant sur des fonctionnalités de transformation (par exemple, XQuery ou XSLT), de validation (par schéma XSD) et éventuellement de transcodification. »***

8.2	Quels sont selon vous les protocoles d'échanges avec lesquels il sera nécessaire d'être interopérable ?	Tous

- Citons : « ***Le hub d'échanges DEVRAIT s'appuyer en interne sur un middleware de messagerie (MOM) qui garantisse la persistance des messages, la reprise sur incident, la garantie de livraison, le respect du mode transactionnel... »***

Ref	Question	Commentaire
8.3	Cette exigence vous semble-t-elle pertinente ? Quelles alternatives voyez-vous ?	La garantie de ces niveaux de services est nécessaire. Cette garantie peut s'appuyer sur différentes technologies
8.4	Quel système de persistance (SGBD/R, MOM, système de fichier) préconisez-vous pour les échanges asynchrones ?	Au choix de l'opérateur (tiers de télétransmission)

- Citons : « ***La plateforme d'échanges DOIT fournir une base de routage afin de contenir les informations de connexion de chaque destinataire. La plateforme DEVRAIT permettre l'interrogation d'une base de routage externe via une interface d'accès LDAP, UDDI, SQL ou par une API Web Services. Un mécanisme de synchronisation entre un référentiel externe et la base de routage de la plateforme DEVRAIT également être possible.*** »

Ref	Question	Commentaire
8.5	Comment sont propagées les mises à jour des tables de routage entre différents hubs interconnectés ? Faut-il imaginer un protocole de synchro du type de BGP (Border Gateway Protocol) ?	A voir le moment venu.

5 Conclusion

Retenir le standard propriétaire **FAST** de la CDC serait une aberration et nous le justifions aisément :

- *Sur le plan éthique :*

  - ✔ Le principe de libre concurrence devant être respecté, on est trivialement en droit d'attendre que les opérateurs et offreurs de solution aient le souci de se référer à des standards ouverts, publiquement disponibles et non à des solutions qui leur soient propres. La norme FAST doit donc être, de facto, rejetée.

  - ✔ L'utilisation d'une norme propriétaire pour gérer des communications pose des problèmes de transparence. Seule l'utilisation de standards ouverts offre une lisibilité suffisante pour garantir, par exemple, l'absence de diffusion non souhaitée d'informations.

- *Sur le plan technique :*

  - ✔ La norme FAST ne répond pas aux standards et poserait donc vite des problèmes d'interopérabilité au sein de l'UE que ce soit au niveau des formats choisis ou de la possibilité de faire abstraction des plate-formes utilisées,

  - ✔ Les expérimentations menées avec la norme FAST ont été peu concluantes,

  - ✔ La norme FAST compte de nombreuses limitations (couches de transport, routage...),

On observe des problèmes similaires avec la norme **eLink** car celle-ci est propriétaire et donc la majorité des problèmes rencontrés avec la norme FAST (pas de suivi strict des recommandations W3C...) même si, techniquement, elle a moins de défaut.

Le standard **SOAP/ebMS2** est trivialement le plus adapté car :

- ✔ Il répond aux besoins actuels que nous avons identifiés dans cette réponse tout en étant extensible et souple pour combler tout besoin à venir (gestion des attachements ET possibilité d'encapsuler les documents en XML, multiples couches de transport utilisables, ...),
- ✔ Il est ouvert et conforme aux recommandations W3C ISO 15000-2, qui sont, à ce jour, les seules normes reconnues par l'ensemble du tissu industriel européen,
- ✔ Il a été élaboré sous l'égide de OASIS ce qui constitue un gage de pérennité, d'évolutivité et d'interopérabilité,
- ✔ Il n'exclut aucun prestataire du marché car tous peuvent l'exploiter.

Nous concluons donc que, d'un point de vue éthique comme technique, ebMS2 est la seule solution acceptable.