

Référentiel Général d'Interopérabilité RGI

Version 1.0

Organisation du document

Avant-propos

L'avant-propos introduit la problématique de l'interopérabilité et présente les bénéfices attendus du RGI.

Il s'adresse en priorité aux décideurs et responsables des autorités administratives.

Cadre d'interopérabilité

Le cadre d'interopérabilité présente le contexte qui a amené à élaborer le RGI, ainsi que les principes adoptés pour la conception et le périmètre de ce document.

Il s'adresse aux directions et aux maîtrises d'ouvrage des autorités administratives œuvrant dans les domaines de l'organisation et des systèmes d'information.

Guide d'interopérabilité

Le guide d'interopérabilité fixe d'abord les règles d'interopérabilité auxquelles les autorités administratives doivent se conformer, puis présente les normes, standards et bonnes pratiques favorisant l'interopérabilité des échanges.

Il s'adresse plus particulièrement aux chefs de projet, architectes et développeurs travaillant sur des projets relatifs à l'administration électronique.

Avant-propos

Le RGI (Référentiel Général d'Interopérabilité) a pour objectif de guider les autorités administratives dans l'adoption de normes, standards et bonnes pratiques, afin de favoriser l'interopérabilité de leurs systèmes d'information.

Le défaut d'interopérabilité

C'est souvent un défaut d'interopérabilité des systèmes qui met le mieux en évidence le concept et l'intérêt de l'interopérabilité.

Un voyage à Londres permet de constater que l'interface des appareils électriques français n'interopère pas avec l'interface du réseau électrique anglais. Il y a quelques années, un voyage en Espagne était l'occasion de réaliser que l'interface des locomotives françaises n'interopérait pas avec l'interface des voies ferrées espagnoles car l'écartement des roues et des voies était différent.

Le défaut d'interopérabilité existe aussi dans le monde des systèmes d'information. Le 23 septembre 1999, la sonde Mars Climate Orbiter fut détruite à cause d'une erreur de navigation pendant sa mise en orbite autour de Mars. Son entrée dans l'atmosphère martienne, prévue à une altitude de 140-150 km, a finalement eu lieu à seulement 57 km de la surface, entraînant sa destruction par les turbulences et les frottements atmosphériques.

L'enquête a mis en évidence que certains paramètres avaient été calculés par un sous-traitant de la NASA en unités de mesure anglo-saxonnes (livre.seconde) et transmises telles quelles à l'équipe de navigation, qui attendait ces données en unités du système métrique (newton.seconde).

Mars Climate Orbiter était l'une des deux sondes spatiales du programme d'étude météorologique Mars Surveyor, dont le budget s'élevait à 328 millions de dollars.

Comment résoudre un défaut d'interopérabilité ?

Pour que des systèmes interopèrent, leurs interfaces doivent être normalisées. Lorsque de nombreux acteurs sont impliqués pour définir et caractériser les interfaces entre systèmes, il est important d'adopter une approche normative. Cette approche permet par exemple de définir le format d'une prise de courant, l'écartement des rails d'une voie de chemin de fer, une unité de mesure, etc.

Un référentiel d'interopérabilité pour les systèmes d'information

A l'instar de nombreux autres pays, pour favoriser les échanges d'information avec les autorités administratives, l'Etat français a souhaité référencer un certain nombre de normes et standards. Le RGI répond à cet objectif. Il résulte des dispositions de l'ordonnance n° 2005-1516 du 8 décembre 2005 « relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives » par laquelle le législateur a souhaité donner aux autorités administratives un cadre de référence en la matière.

Un nombre volontairement limité de normes et de standards sont posés sous forme de règles et constituent donc un tronc commun technique sur lequel les autorités administratives doivent s'aligner, selon les dispositions prévues par l'article 11 de l'ordonnance n° 2005-1516 du 8 décembre 2005.

Le nombre de règles du RGI est réduit afin de limiter l'impact de la mise en conformité des SI (Systèmes d'Information). Au-delà du référencement de ces règles qui font largement consensus, le RGI a également pour but de guider les autorités administratives en mettant en lumière :

- des normes et standards qui sont le reflet de bonnes pratiques d'interopérabilité mais qui ne sont pas encore adoptés par l'ensemble des parties prenantes ; ces normes et standards font l'objet de recommandations ;
- des normes et des standards qui disposent d'un fort potentiel en terme d'interopérabilité mais qui, pour un déficit de maturité ou d'adoption par le marché, ne sont pas encore éligibles au rang de recommandations; ces normes et standards sont alors placés « en observation ».

Portant sur des technologies en évolution constante, le RGI est un document vivant et qui connaîtra des actualisations régulières. La présente version expose l'état actuel des questions d'interopérabilité à une date donnée. Cette première version du RGI, et tout particulièrement le guide d'interopérabilité, sont destinés à appuyer les autorités administratives dans leurs choix techniques afin de développer l'interopérabilité. Cependant la mise en conformité des échanges d'information aux normes, standards et bonnes pratiques recommandés ou placés en observation reste à l'entière discrétion de chaque autorité administrative.

Les dix bénéfiques attendus du RGI

1 - Améliorer la qualité des services fournis aux administrés

En permettant la mise en œuvre de services transverses et interactifs, l'interopérabilité des SI s'impose comme un accélérateur du développement de l'administration électronique.

Cette évolution vers une administration modernisée permet de répondre aux exigences croissantes des citoyens en termes de qualité de service, c'est-à-dire un accès simplifié via différents canaux, un traitement individualisé et une réduction du cloisonnement administratif.

2 - Promouvoir les services en ligne en réduisant les délais de mise en œuvre

L'adoption de normes et standards communs au sein de l'administration accélère les phases de conception et d'intégration tout en favorisant la réutilisation de composants.

La réduction des délais liée à la standardisation des échanges permet d'accélérer la mise en œuvre de services en lignes entre administrations.

3 - Maîtriser les coûts de développement et de maintenance

Le défaut d'interopérabilité a un coût : le coût de l'incompréhension entre agents n'utilisant pas les mêmes termes pour désigner les mêmes choses, le coût de

transformations sémantiques pour que deux administrations parlent le même langage, le coût de mise en place de plateformes d'échanges pour transporter mais aussi transformer les flux entre SI, le coût de développement d'interfaces entre applications, le coût de maintenance des paramétrages et des développements, etc.

Le RGI propose une sémantique commune à l'ensemble des échanges entre administrations et des "connexions" logicielles communes pour l'ensemble des SI de l'Etat. Il permet aussi de maîtriser les coûts de développement et de maintenance des SI.

4 - Favoriser l'interopérabilité des systèmes d'information en respectant l'autonomie des acteurs

Le RGI définit un cadre de recommandations référençant des normes et standards qui favorisent l'interopérabilité au sein des SI de l'administration.

Ces recommandations constituent les objectifs à atteindre pour favoriser l'interopérabilité. Les moyens d'y parvenir sont à la discrétion des responsables des SI de l'administration, en fonction de leurs propres enjeux, de leur planning et du rapport entre le coût de mise en œuvre et les bénéfices attendus.

5 - Contribuer à l'ouverture des systèmes d'information dans leur écosystème (relations avec les citoyens et les entreprises et avec d'autres organismes publics)

Dans un contexte marqué par l'intensification des relations en ligne entre les services de l'Etat et les citoyens, par le besoin d'améliorer la qualité des services et la performance des administrations, et par l'émergence de nouveaux services rendus par Internet au public, les SI doivent adapter leurs propres capacités d'ouverture et d'échanges.

Il ne s'agit plus tant, aujourd'hui, de refondre les SI, que d'améliorer leurs échanges en développant leur interopérabilité, c'est-à-dire leur capacité à fonctionner avec d'autres systèmes.

6 - Adopter un langage et une sémantique communs lors des échanges d'information

L'utilisation d'un langage commun, d'une terminologie commune et de procédures communes aux différents acteurs (usagers, administrations) aide ceux-ci à mieux se comprendre, à mieux communiquer et à mieux échanger.

Dans le domaine de l'interopérabilité, cette recherche d'un langage commun concerne uniquement les données échangées entre systèmes ; les données internes à un système ne sont pas concernées par l'interopérabilité. L'interopérabilité sémantique est le résultat d'un accord entre les différents acteurs d'un processus. Ils adhèrent à un langage commun dans un périmètre métier prédéfini.

7 - Diffuser les bonnes pratiques entre administrations européennes et converger vers un cadre d'interopérabilité commun

Près d'une quinzaine de pays européens ont déjà développé ou sont en train de développer leur cadre d'interopérabilité. La Commission européenne développe également le cadre d'interopérabilité EIF (*European Interoperability Framework*) pour les applications transfrontalières.

Travailler en coordination avec les autres Etats membres et en conformité avec l'EIF permet d'élaborer des services administratifs transfrontaliers. Le panel d'offres de services est potentiellement vaste : la délivrance de permis de travail, permis de séjour, certificats de naissance, diplômes universitaires et visas ; les déclarations d'impôts, de marchandises sous douane et de TVA ; ou encore l'enregistrement de marques, de brevets, etc.

Ces services s'adressent aux citoyens et aux entreprises d'un même Etat, aux citoyens et aux entreprises d'un autre Etat membre de l'Union Européenne, aux administrations d'un même Etat ou encore aux administrations d'un autre Etat membre de l'Union Européenne.

8 - Favoriser l'intégration et guider les administrations dans leurs choix de solutions

L'adoption d'un cadre d'interopérabilité permet à une administration de potentiellement intégrer son SI sans couture et sans interfaces compliquées au SI de toute autre administration ayant adopté les mêmes "connecteurs".

La conformité à un ensemble de normes et de standards référencés dans le RGI peut s'exprimer sous la forme de besoins dans un cahier des charges et constituer un élément de décision lors du choix d'une solution applicative ou technique.

9 - Garantir la neutralité de l'administration en s'appuyant sur des normes et standards

L'administration doit s'assurer que les solutions et/ou les produits qu'elle acquiert sont sélectionnés au cours d'un processus garantissant la libre concurrence. En outre, il est important que les choix de l'administration puissent se porter sur les meilleurs produits et services correspondant à ses besoins spécifiques du moment, tout en laissant libre de ses choix futurs.

C'est pourquoi les normes et les standards préconisés dans le RGI ne concernent que les échanges entre SI ou applications et n'imposent aucune solution technique.

En effet, lorsqu'une administration échange des documents avec une autre administration, des entreprises ou des citoyens, cet échange doit reposer sur un minimum de connectivité sans rendre obligatoire l'utilisation d'un produit logiciel ou matériel.

10 - Favoriser la standardisation et l'innovation

La référence à des normes et standards externes permet aux partenaires d'un échange d'aller au-delà de simples arrangements bilatéraux, de réutiliser des spécifications existantes et donc de limiter les coûts liés à la réalisation de solutions spécifiques.

La stratégie européenne pour la croissance et l'emploi précise qu'une standardisation forte et dynamique est un des instruments pour encourager l'innovation. Elle considère la standardisation comme d'intérêt public, en particulier lorsque la sécurité, la santé, l'environnement et les performances sont en jeu (cf. EIF).

Précisions importantes

Le RGI ne crée pas de normes

Le RGI est un référentiel ; il référence des normes et standards reconnus et s'appuie pour cela sur les travaux des organismes de normalisation.

Le RGI ne traite pas de l'architecture d'un SI

Le périmètre du RGI concerne les capacités d'un SI à échanger avec d'autres SI et ne couvre ni l'architecture d'un SI, ni son fonctionnement interne.

Le RGI ne fixe pas de règles relatives à des solutions

Les règles du RGI concernent le recours à des normes, standards ou bonnes pratiques destinés à améliorer l'interopérabilité des SI. Le RGI ne préconise pas de solutions logicielles ou techniques.

Le RGI n'est pas exhaustif dans ses préconisations

Le RGI préconise un certain nombre de normes, standards et bonnes pratiques répondant en priorité aux besoins actuels des utilisateurs. Aucune norme, ni aucun standard n'est interdit, ni déconseillé.

Partie 1 : Cadre d'interopérabilité

Sommaire du cadre d'interopérabilité

1 - CONTEXTE ET ENVIRONNEMENT	10
2 - DEMARCHE D'ELABORATION.....	11
3 - DOMAINES D'INTEROPERABILITE.....	15
4 - PRESENTATION DES NIVEAUX D'INTEROPERABILITE.....	17
5 - EVOLUTION DU DOCUMENT.....	20
6 - MODALITES D'APPLICATION DU RGI	21

1. Contexte et environnement

1.1. L'administration en ligne

Le développement de l'administration en ligne a profondément modifié les relations entre les usagers, les agents publics et les autorités administratives.

Pour accompagner ce développement, les autorités administratives doivent proposer un environnement de travail interopérable, favorisant la collaboration. Cet environnement doit également garantir les éléments suivants :

- Protection de la vie privée,
- Respect de l'anonymat,
- Egalité d'accès aux services,
- Transparence de l'administration,
- Droits d'accès aux données nominatives et aux services,
- Disponibilité des services,
- Authenticité et opposabilité des actes dématérialisés.

Tous ces éléments contribuent à apporter la confiance nécessaire au développement de l'administration électronique, au sein des administrations, entre les administrations et les entreprises, ainsi qu'entre les administrations et les citoyens.

Afin d'assurer les échanges entre les différents acteurs de l'administration électronique, il est nécessaire pour ces derniers d'adopter un langage commun. Le RGI a été élaboré pour répondre à cette préoccupation.

1.2. Cadre législatif

Le RGI résulte des dispositions de l'ordonnance n° 2005-1516 du 8 décembre 2005 et du décret n° 2007-284 du 2 mars 2007.

L'ordonnance n° 2005-1516 est relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. Elle s'inscrit dans une démarche globale de modernisation de l'Etat et plus précisément dans une logique de simplification des démarches des usagers et de facilitation de l'accès de ces derniers aux services publics.

L'article 11 de cette ordonnance introduit la notion de Référentiel Général d'Interopérabilité : « *L'objet du RGI est de fixer les règles techniques permettant d'assurer l'interopérabilité de tout ensemble de moyens destinés à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives* ».

L'article 14 fixe quant à lui les conditions de mise en conformité. Les systèmes existants au moment de la publication se mettent en conformité dans les trois ans, les applications créées dans les six mois suivants au plus tard douze mois après.

2. Démarche d'élaboration

2.1. Démarche et partis pris

L'approche adoptée pour l'élaboration du RGI repose sur les principes suivants :

- Le document proposé à la lecture se veut utile et facile à consulter ;
- Le document fait référence à des normes et standards reconnus ; il s'appuie sur les travaux réalisés par les organismes de normalisation ;
- Le référencement des normes et standards est appuyé sur des critères d'adoption explicités dans le document ; ces critères reposent sur la méthode d'évaluation des normes et standards élaborée par la Commission Européenne : CAMSS (Common Assessment Method for Standards and Specifications) ;
- Le périmètre du document est l'interopérabilité ; le document n'est pas un recueil de solutions techniques, ni un manuel d'architecture, ni un guide d'implémentation ;
- Le RGI concerne l'ensemble des autorités administratives, c'est-à-dire les collectivités locales, les organismes publics et les services de l'Etat; aussi, le niveau d'exigence traduit dans les règles du RGI doit être adapté à l'ensemble des autorités administratives.

2.2. Démarche de sélection des normes et standards

2.2.1. Normes et standards

Pour la compréhension du RGI les définitions suivantes de « norme » et « standard » sont à utiliser.

Standard : modèle de référence adopté par l'usage d'un groupe de personnes.

Norme : document de référence fixant les conditions dans lesquelles une opération est réalisée, un objet exécuté, un produit élaboré, avec deux caractéristiques fondamentales :

- émaner des organismes officiels de normalisation (les organismes sont présentés dans le chapitre 2.3),
- être à la fois le fruit du consensus de l'ensemble des acteurs et le résultat du transfert du savoir-faire de ces acteurs.

2.2.2. Critères d'adoption retenus

Les normes et standards présentés ont été sélectionnés selon leur pertinence par rapport aux trois critères ci-dessous, issus de la méthode d'évaluation CAMSS :

Ouverture

- Les spécifications techniques de la norme ou du standard sont publiques et sans restriction d'accès ni de mise en œuvre,
- La norme ou le standard a été adopté par un organisme de normalisation.

En effet, il est souhaitable qu'une norme ou un standard soit ouvert et puisse être implémenté par une multitude de solutions logicielles. L'ouverture permet ainsi de garantir l'indépendance vis-à-vis des fournisseurs et de laisser le choix de leurs outils aux parties prenantes. La libre disponibilité des spécifications permet, de plus, d'assurer un accès à long terme aux données.

Potentiel d'évolution

- Les spécifications évoluent dans les temps, avec l'ajout de nouvelles fonctionnalités,
- Un calendrier d'évolutions est publié et les utilisateurs sont informés de la teneur des prochaines versions,
- La norme ou le standard présente la stabilité nécessaire et les nouvelles versions doivent prendre en compte au moins les problématiques de compatibilité ascendante.

Les normes et standards doivent évoluer afin de proposer des fonctionnalités adaptées aux besoins des utilisateurs, tout en garantissant des mécanismes natifs de compatibilité entre leurs différentes versions, afin d'assurer l'interopérabilité entre leurs utilisateurs.

Adoption par le marché

- La norme ou le standard dispose d'une part de marché significative,
- La norme ou le standard est implémenté par plusieurs éditeurs logiciels,
- De l'expertise autour de l'implémentation et de la maintenance sont proposées par de nombreux prestataires,
- Du fait de sa maturité, de nombreux supports d'aide à l'implémentation et à la maintenance sont disponibles et les meilleures pratiques sont identifiées.

L'adoption par le marché reflète à la fois l'industrialisation de la norme ou du standard, son taux d'adoption par les utilisateurs et la facilité à disposer d'assistance.

Selon la maturité et l'écosystème des domaines et thèmes étudiés, le poids des critères peut se révéler différent. Il faut également noter que la non-adhérence à un critère n'est pas éliminatoire. Le RGI cherche à faire preuve de pragmatisme et propose pour chaque thème spécifique une liste de normes et standards répondant au mieux aux critères.

2.3. Organismes de normalisation

Les organismes de normalisation sont des entités qui travaillent à l'établissement et au maintien de normes et dont les membres peuvent être des personnes publiques ou privées.

Les organisations officielles mondiales de normalisation sont :

- ISO : Organisation Internationale de Normalisation,
- CEI : Commission Electrotechnique Internationale,
- UIT : Union Internationale des Télécommunications,
- UN/CEFACT : *United Nations Centre for Trade Facilitation and Electronic Business* ou centre de facilitation du commerce et des transactions électroniques,
- ETSI : *European Telecommunications Standards Institute* ou Institut européen des normes de télécommunication.

En dehors des technologies de l'information et de la communication, une partie importante de la normalisation mondiale est organisée autour des structures ISO et CEI, qui fonctionnent sur le principe de délégations nationales.

Pour participer à leurs activités les acteurs économiques des pays doivent disposer d'une organisation nationale de normalisation, canal incontournable pour porter les positions des acteurs nationaux (privés ou publics). Le fonctionnement de cette organisation est souvent placé sous la tutelle de l'État, comme c'est le cas pour l'AFNOR (Association Française de NORmalisation) en France.

Au niveau communautaire, le CEN (Comité Européen de Normalisation) et le CENELEC (Comité Européen de Normalisation ELECTrotechnique) fonctionnent selon le modèle des délégations nationales de l'ISO et la CEI, dont ils constituent souvent un relais.

Le domaine des technologies de l'information et de la communication concerne toutes les organisations mais relève principalement de l'UIT, du CEFACT et de l'ETSI. Ce dernier est aussi, conjointement avec le CEN et le CENELEC une des trois organisations reconnues par l'Union européenne.

Pour fonctionner, le CEN et le CENELEC s'appuient principalement sur les états, tandis que l'ETSI s'appuie directement sur ses membres qui peuvent être des acteurs privés ou publics. Le Ministère de l'Economie de l'Industrie et des Entreprises (MEIE) invite tous les acteurs concernés à des concertations sur une base de réunions régulières. En pratique l'implication directe des acteurs privés y est importante.

En complément des organisations officielles, le secteur des technologies de l'information et des télécommunications se caractérise par un foisonnement d'organismes qui contribuent à l'évolution des standards.

Les principaux organismes menant des travaux relatifs aux échanges électroniques sont les suivants :

- OASIS : Organization for the Advancement of Structured Information Standards,
- W3C : World Wide Web Consortium,
- IETF : Internet Engineering Task Force,
- ECMA : European Computer Manufacturers Association,
- OMG : Object Management Group,
- WS-I : Web Services Interoperability Organisation.

3. Domaines d'interopérabilité

3.1. Périmètre de l'interopérabilité

Le RGI traite de l'interopérabilité entre :

- Les autorités administratives : $A \leftrightarrow A$,
- Une autorité administrative et une entreprise : $A \leftrightarrow B$,
- Une autorité administrative et un citoyen : $A \leftrightarrow C$.

Note : A recouvre la notion d'autorité administrative
 B (Business) recouvre la notion d'entreprise
 C recouvre la notion de citoyen

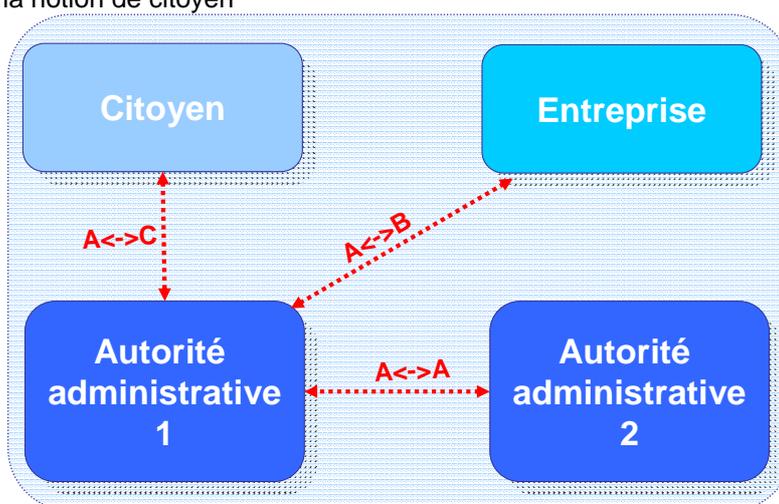


Figure 1 : Périmètre du RGI

Pour leurs besoins internes, les autorités administratives restent libres du choix des normes, standards et pratiques à mettre en œuvre.

Le cadre français d'interopérabilité doit également s'intégrer dans le contexte européen, défini par les travaux de l'EIF, dont le périmètre est présenté Figure 2.

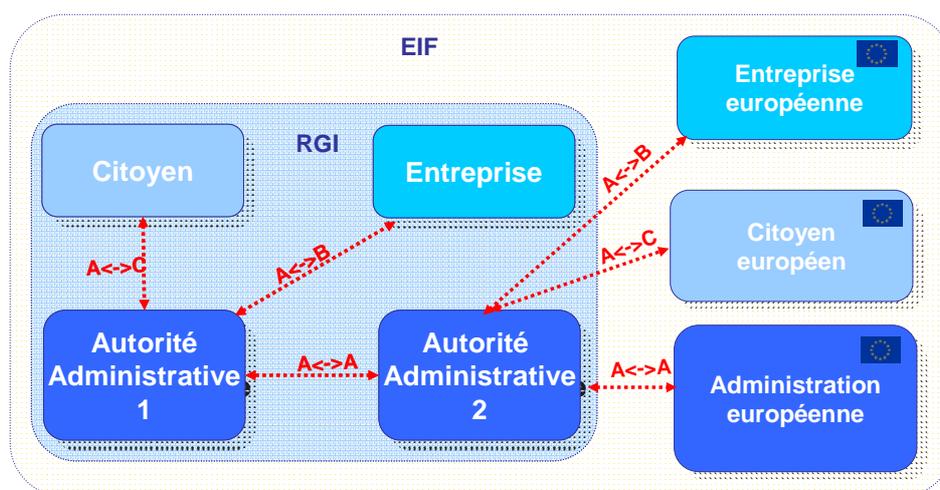


Figure 2 : Périmètre européen

L'objectif de l'EIF est de favoriser le développement de services en ligne européens (EPS pour *European Public Services*), en facilitant la coopération entre les administrations des différents Etats Membres. Le cadre européen propose des recommandations et bonnes pratiques aux niveaux organisationnel, sémantique et technique.

La Commission Européenne recommande à tous les Etats Membres d'aligner leur cadre d'interopérabilité respectif sur le cadre européen EIF. Un observatoire des cadres nationaux NIFO (*National Interoperability Framework Observatory*) a été mis en place afin, entre autres, de faciliter cet alignement.

3.2. Typologie des acteurs concernés

Différents types d'acteurs prennent part aux échanges couverts par le périmètre du RGI :

- Le terme « *usager* » recouvre les notions :
 - d'*usager - citoyen*, personne physique,
 - d'*usager - entreprise*, personne morale,
- L'agent public, personne physique agissant au nom d'une autorité administrative,
- Le SI d'une entreprise, entité technique,
- Le SI d'une autorité administrative, entité technique.

4. Présentation des niveaux d'interopérabilité

4.1. Les différents niveaux d'interopérabilité

Un échange réussi entre parties prenantes nécessite la prise en compte de différents niveaux d'interopérabilité.

Le schéma présenté en Figure 3 s'inspire du modèle proposé dans l'EIF. Il est constitué de six niveaux :



Figure 3 : Les six niveaux d'interopérabilité

- **Niveau politique**
Des visions partagées et des stratégies convergentes favorisent les échanges entre parties prenantes.
- **Niveau juridique**
Les échanges doivent se conformer :
 - au cadre légal dont dépendent les parties prenantes (droit national et international, propriété intellectuelle, confidentialité, etc.) ;
 - aux accords contractuels établis entre parties prenantes (modalités de l'échange, niveaux de services, etc.).
- **Niveau organisationnel**
L'interopérabilité organisationnelle est liée aux organisations et aux moyens mis en œuvre pour favoriser les échanges.

En termes d'organisation, il s'agit par exemple de définir les rôles et les responsabilités des personnes au sein de leur entité qui prennent part à l'échange.

En termes de moyens, il s'agit de mettre en place les ressources, notamment informatiques, qui vont sous-tendre les échanges.

- **Niveau sémantique**
La sémantique recouvre à la fois la signification des mots et le rapport entre le sens des mots (homonymie, synonymie, etc.). Le sens des mots varie selon les organisations, les métiers, les acteurs et les contextes. Toute collaboration entre entités demande une communication, au sens échanges d'informations. Pour cela, ces entités s'entendent sur la signification des données qu'elles échangent.
- **Niveau syntaxique**
La syntaxe traduit le sens en symboles.
Il y a entre la sémantique et la syntaxe le même rapport qu'entre le fond et la forme.
- **Niveau technique**
Le niveau technique véhicule les informations définies au niveau sémantique et mises en forme au niveau syntaxique.

4.2. Les niveaux d'interopérabilité traités par le RGI

Il n'est pas du ressort du RGI de traiter de l'interopérabilité politique, juridique ou organisationnelle.

Le périmètre de l'interopérabilité couvert par le RGI s'étend de la compréhension entre les acteurs qui échangent jusqu'à la mise en œuvre technique qui permet aux systèmes de communiquer entre eux. Il concerne donc (voir Figure 4) :

- L'interopérabilité sémantique : « savoir se comprendre »,
- L'interopérabilité syntaxique : « savoir communiquer »,
- L'interopérabilité technique : « pouvoir communiquer ».

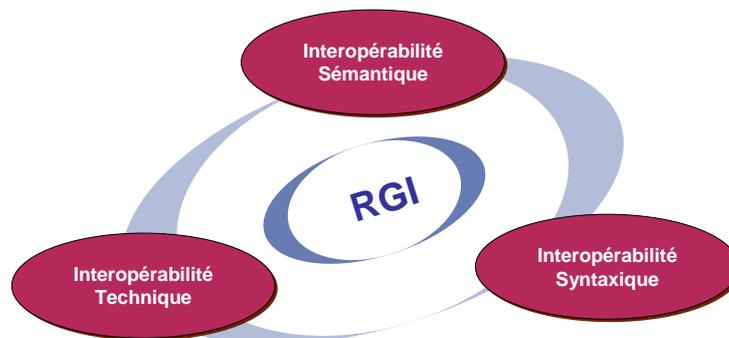


Figure 4 : Les trois niveaux d'interopérabilité du RGI

Pour ces trois niveaux d'interopérabilité, le RGI propose un certain nombre de normes, standards et pratiques qui peuvent être privilégiés lors des échanges d'information, afin que les différentes parties prenantes des échanges puissent lire, manipuler et conserver ces informations.

4.2.1. Les domaines de l'interopérabilité sémantique

Dans le RGI, l'interopérabilité sémantique est divisée en trois domaines :

- La conception des échanges
Il s'agit de décrire les concepts de l'échange et une démarche générique permettant d'analyser les échanges.
- Les méthodes et les langages de spécification
Le RGI recommande méthodes et langages permettant de formaliser les échanges.
- Les ressources sémantiques pouvant être réutilisées
Le RGI répertorie les ressources sémantiques susceptibles d'être utilisées lors de la conception des échanges.

4.2.2. Les domaines de l'interopérabilité syntaxique

L'interopérabilité syntaxique concerne la façon dont sont codées et formatées les données. Dans le RGI, elle est divisée en deux domaines :

- Les formats élémentaires
Les formats élémentaires incluent les formats pour le son, la photo, l'image animée et le codage des caractères.
- Les formats composites
Les formats composites sont des agrégats de plusieurs objets et incluent par exemple, les documents bureautiques ou les formats de compression de fichiers.

4.2.3. Les domaines de l'interopérabilité technique

Le RGI regroupe les normes et standards techniques selon quatre grands domaines :

- La présentation
La présentation traite des technologies de navigation et de restitution.
- Le multimédia
Le multimédia traite des technologies de communication entre humains, notamment de la messagerie et de la téléphonie.
- Les services web
Les services web traitent des technologies d'échanges entre SI.
- L'infrastructure
L'infrastructure traite des technologies élémentaires nécessaires aux échanges, notamment des protocoles réseau.

5. Evolution du document

Les conditions d'élaboration, d'approbation, de modification et de publication du RGI sont fixées par décret. Ceci se traduit notamment par :

- la publication du document sur un site Web public, afin qu'il soit consultable par tous,
- des mises à jour régulières, afin de tenir compte des évolutions des technologies et des usages des autorités administratives.

6. Modalités d'application du RGI

A l'instar de nombreux autres pays, pour favoriser les échanges d'information avec les autorités administratives, l'Etat français a souhaité référencer un certain nombre de normes et standards. Le RGI répond à cette préoccupation. Il résulte des dispositions de l'ordonnance n° 2005-1516 du 8 décembre 2005 « relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ».

Les normes et les standards exprimés sous forme de règles constituent un tronc commun technique minimal sur lequel les autorités administratives doivent s'aligner, selon les dispositions prévues par l'article 11 de l'ordonnance.

Au-delà du référencement de ces règles qui font largement consensus, le RGI a également pour objectif de guider les autorités administratives en mettant en lumière :

- des normes et standards qui sont le reflet de bonnes pratiques d'interopérabilité mais qui ne sont pas encore adoptés par l'ensemble des parties prenantes ; ces normes et standards font l'objet de recommandations ;
- des normes et des standards qui disposent d'un fort potentiel en terme d'interopérabilité mais qui, pour un déficit de maturité ou d'adoption par le marché, ne sont pas encore éligibles au rang de recommandations; ces normes et standards sont placés « en observation ».

Le nombre de règles reprises dans le tronc commun technique minimal est volontairement réduit afin de limiter l'impact de la mise en conformité des SI. Ces règles peuvent être consultées sur les fiches thématiques suivantes :

Fiches thématiques concernant la messagerie :

- les [protocoles de messagerie](#), page 75
- la [représentation des messages et des pièces jointes](#), page 76
- la [sécurisation de la messagerie](#), page 77
- l'[accès aux boîtes aux lettres électroniques](#), page 78

Fiche thématique concernant les [profils de Services Web](#), page 91

Fiches thématiques concernant l'infrastructure :

- les [annuaires LDAP](#), page 95
- le [service de noms de domaine](#), page 98
- le [protocole réseau](#), page 101
- les [protocoles de transport](#), page 102
- le [protocole client-serveur](#), page 103
- les [meilleures pratiques HTTP](#), page 105
- le [service de sécurisation des échanges](#), page 108
- l'[Horodatage et synchronisation](#), page 110

Cas particulier faisant l'objet d'un accord bilatéral :

Si deux entités ont choisi, d'un commun accord l'utilisation d'un protocole ou d'un format pour un échange limité à elles-mêmes, elles pourront continuer à échanger selon ces modalités, tant que ce choix n'affecte pas les échanges avec d'autres acteurs.

Partie 2 : Guide d'interopérabilité

Sommaire du guide d'interopérabilité

1 - STRUCTURE DU GUIDE D'INTEROPERABILITE	24
2 - INTEROPERABILITE SEMANTIQUE	27
3 - INTEROPERABILITE SYNTAXIQUE	50
4 - INTEROPERABILITE TECHNIQUE.....	70
5 - GLOSSAIRE	111
6 - GESTION DES VERSIONS.....	117
SOMMAIRE DETAILLE.....	118

1. Structure du guide d'interopérabilité

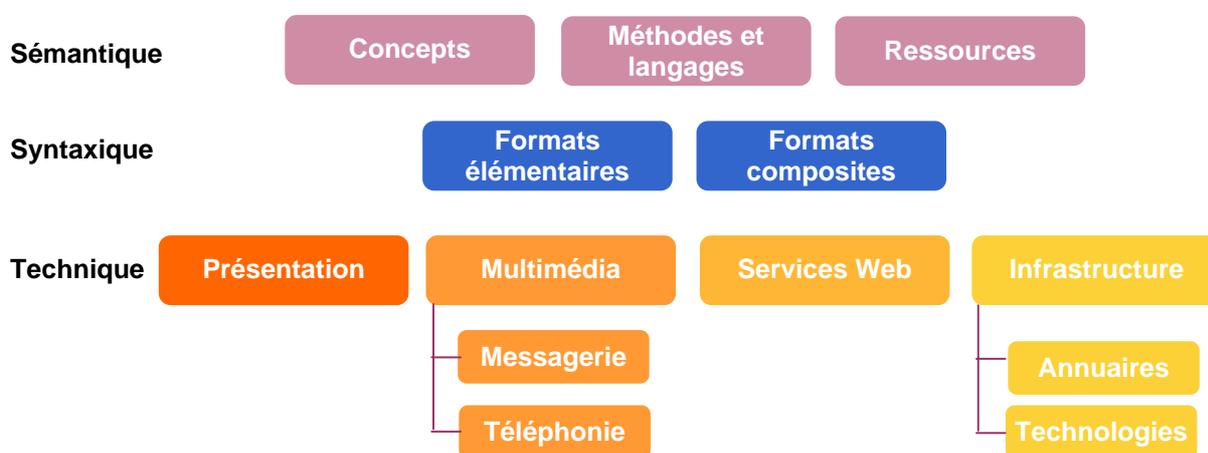
1.1. Guide d'interopérabilité

Le guide d'interopérabilité est composé de fiches thématiques, présentées selon les trois niveaux d'interopérabilité traités par le RGI :

- Sémantique,
- Syntaxique,
- Technique.

Les chapitres dédiés à chaque niveau reprennent les domaines introduits précédemment, ces derniers regroupant plusieurs thèmes connexes.

Cliquez sur les domaines afin de les consulter



1.2. Présentation des règles d'interopérabilité

Les règles d'interopérabilité sont présentées de la manière suivante :

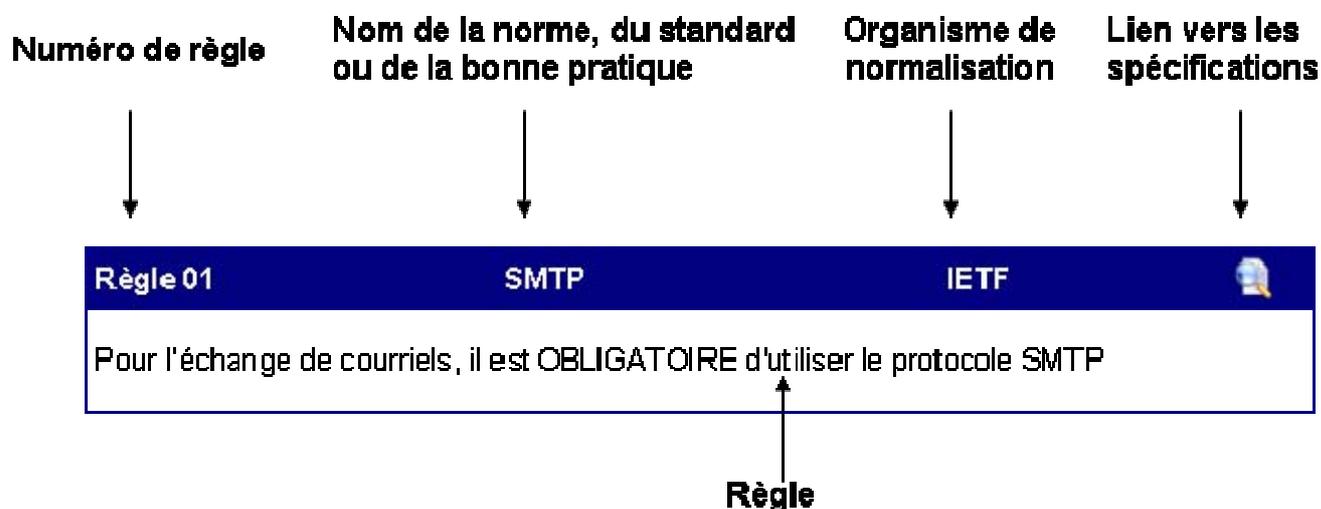


Figure 5 : Représentation des règles RGI

Les normes, standards ou bonnes pratiques faisant l'objet de recommandations ou étant mis en observation reprennent cette charte de présentation, tout en adoptant des codes couleurs différents.

Dans le cas de bonnes pratiques, les organismes de normalisation et les liens vers les spécifications ne sont pas indiqués.

Des liens vers des problématiques connexes peuvent également être proposés dans certains chapitres du guide d'interopérabilité.

Exemple :



Concernant la sécurisation des communications échangées, XMPP utilise le protocole TLS. Ce protocole est détaillé au chapitre 4.4.2.8 *Service de sécurisation des échanges*

1.3. Liste des normes et standards référencés

Cliquez sur les normes et standards afin de consulter le(s) thème(s) associé(s)

A	Atom Publishing				
B	Basic Security Profile BPMN				
C	CGM	CSS	CSV		
D	DCF77	DNG	DNS	DNSsec	DSML
E	ECMAScript	ESMTP	ESMTP STARTTLS		
F	Flac	FTP			
G	G.168	G.711A	G.722	G.723.1	G.729
	G.729.A	GIF	GSM 06.10		
H	H.323	HTML	HTTP	HTTP POST	
I	iLBC	ID-WSF	IMAP4	IPsec	IPv4
	IPv6				
J	JPEG	JSON			
L	LDAP	LDIF	'literal'		
M	MDC	MIME	MP3 (1 2)	MPEG-2	MPEG-4
N	Navigateurs	NTP			
O	ODF	Ogg-Vorbis	Open XML	OpenDWG	
P	PDF 1.7 (1 2 3)	PDF/A	PDF/X	PNG	Polices d'écriture
	POP3	PRESTO			
R	RSS	RTCP	RTP (1 2)	RTSP	
S	S/MIME	SAML	SCTP	SFTP	SIP
	SMTP	SOAP	Speex	SSL	
	SVG				
T	TCP	TDF	TIFF	TLS	
U	UDDI	UDP	UML	UN/CEFACT	UTC
	UTF-8				
W	WAV	WSDL	WS-I Attachments	WS-I Basic Profile	WSRP
	WS-Security				
X	X3D	XHTML	XMI	XML (1 2)	
	XML Schema	XMPP	XPath	XSLT	
Z	ZIP				

2. Interopérabilité sémantique

2.1. Introduction

La sémantique est une branche de la linguistique qui étudie le sens des mots. Le mot sémantique a été inventé au XIX^{ème} siècle par le linguiste français Michel Bréal, auteur du premier traité de sémantique.

La sémantique recouvre à la fois la signification des mots et le rapport entre le sens des mots (homonymie, synonymie, ...).

Toute collaboration entre entités demande une communication, au sens échanges d'informations. Pour cela, ces entités s'entendent sur la signification des données qu'elles échangent.

L'interopérabilité sémantique caractérise la capacité à s'accorder sur :

- le contexte de l'échange,
- le processus de l'échange,
- le sens et la structuration de l'information échangée.

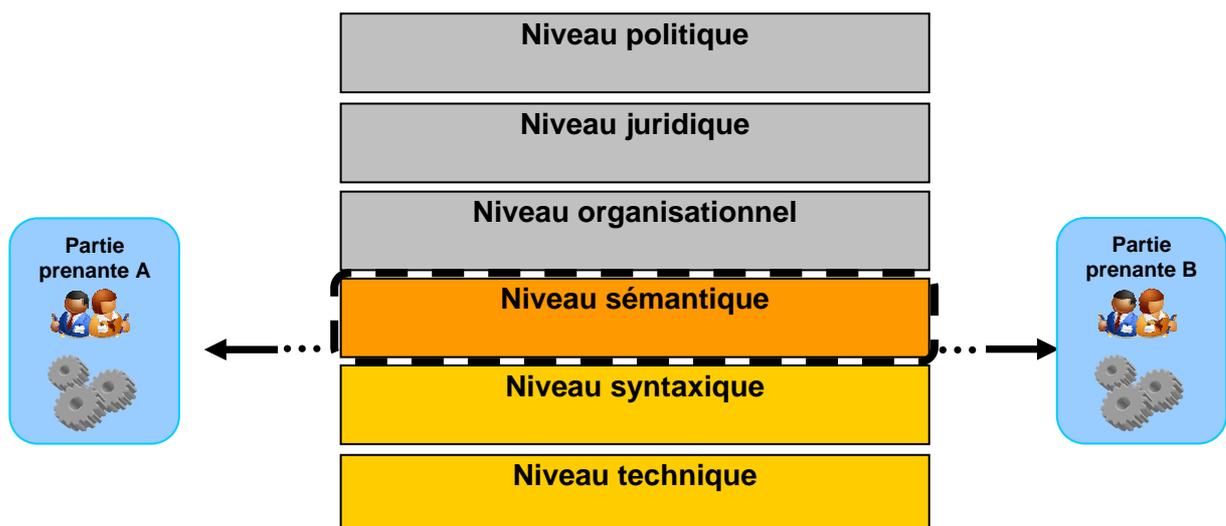


Figure 6 : le niveau sémantique traite du sens de l'information

Le niveau sémantique traite du sens des informations (voir Figure 6) et se distingue en cela du niveau syntaxique relatif à la façon dont les données sont codées et formatées.

Le sens des mots varie selon les organisations, les métiers, les acteurs et les contextes. Lorsque deux parties prenantes (expéditeur, destinataire) décident d'échanger, elles s'exposent à des conflits d'ordre sémantique. Leurs conséquences, de différentes natures, peuvent être importantes comme celles financières révélées sur le projet Mars Climate Orbiter, cité en avant-propos.

Voici quelques exemples courants de conflits sémantiques :

- L'expéditeur et destinataire de l'échange utilisent des identifiants différents pour désigner le même produit (synonymie);
- l'identifiant du produit expédié correspond chez le destinataire à l'identifiant d'un autre produit (homonymie);
- l'expéditeur consent une réduction des frais d'envoi en France et considère que le mot France recouvre la France métropolitaine alors que le destinataire considère que le mot France intègre les DOM et les TOM;
- pour catégoriser les produits vendus, l'expéditeur utilise une table de codes différente de celle du destinataire ;
- sans indication de la devise, l'expéditeur pense émettre un montant en dollars alors que le montant est attendu par le destinataire en euros.

L'anticipation de ces conflits est du ressort des parties prenantes de l'échange. Ils doivent être pris en compte de préférence dès la conception des échanges et non au moment de la mise en œuvre technique.

Pour que les systèmes d'information soient interopérables, les noms, attributs, valeurs, listes de codes qui entrent dans le périmètre de leur collaboration, doivent être harmonisés. L'étude de l'interopérabilité sémantique doit donc débuter par une ontologie partagée, c'est-à-dire une entente entre les parties prenantes sur les concepts manipulés et leurs liens.

Ce document:

- présente la conception des échanges,
- décrit les méthodes de spécifications et les langages
- indique les ressources sémantiques à réutiliser.

2.2. Conception des échanges

Cette partie présente les concepts relatifs aux échanges et une démarche générique pour concevoir ces échanges.

2.2.1. Les concepts de base liés aux échanges

Une définition aboutie d'un échange passe par l'étude de son contexte, de son processus, des acteurs impliqués et des objets qui "circulent" d'un acteur à l'autre.

Le contexte

Le contexte dicte son sens au mot. Par exemple, une personne est désignée comme un "patient" ou un "agent", selon qu'elle est perçue dans un contexte "santé" ou "administration".

Le processus

Selon ISO 9000, un processus est «un ensemble d'activités corrélées ou interactives qui transforme des éléments d'entrée en éléments de sortie ». Il peut être considéré comme un ensemble organisé d'activités, déclenché par un évènement. Il utilise des ressources (personnel, équipement, matériels et machines, matière première et informations) pour transformer des objets en entrée en objets en sortie.

Les processus mettant en œuvre des échanges de données entre parties prenantes sont appelés processus d'échanges ou encore processus collaboratifs.

L'acteur

Un acteur est une organisation ou une personne impliquée en tant que partie prenante dans un processus d'échange.

L'objet ou classe d'objets

On nomme « objet » la représentation de ce qui est partagé par les parties prenantes dans un contexte donné. Par exemple, dans un contexte d'échange d'informations fiscales, "foyer fiscal" ou "contribuable" peuvent être des objets.

L'objet peut être matériel (un produit reçu ou expédié) ou immatériel (un compte bancaire, une commande). Un objet est identifiable, caractérisé par des propriétés (prénom, code postal,...) et des liens avec d'autres objets.

Une classe est une abstraction d'objets ayant des caractéristiques communes. Une classe est décrite par :

- une définition ;
- un nom déduit de sa définition ;
- des attributs; par exemple, la classe "Produit" peut posséder les attributs "Couleur", " Poids", "Texture", etc. Ces attributs sont caractérisés par des types (code, montant, texte, etc.) ;
- des relations avec d'autres classes; cette caractéristique apporte une information complémentaire, par exemple, à la classe "Produit" peuvent être associées les classes "Fournisseur" et "Point de vente".

2.2.2. Une démarche générique de conception des échanges

Ce chapitre présente, dans les grandes lignes, une démarche générique permettant de concevoir les échanges d'informations entre parties prenantes jusqu'à la transformation syntaxique.

La démarche couvre seulement les exigences fonctionnelles liées aux échanges. Elle ne prend pas en compte les exigences non fonctionnelles telles que les volumes, la fréquence et les aspects de sécurité de ces échanges.

Elle ne couvre pas l'architecture de la solution (intégration dans le système d'information, technologies utilisées), ni son implémentation (développement, tests, etc).

Cette formalisation des échanges d'informations s'appuie sur des langages de modélisation. Quel que soit le modèle présenté dans la suite du document, il ne se résume jamais à un dessin. La sémantique du modèle est apportée par les descriptions textuelles des éléments modélisés. Elles doivent être claires et partagées par les parties prenantes de l'échange. Et quel que soit le mode de formalisation choisi, il est recommandé de définir et répertorier dans un glossaire, tous les termes utilisés au fur et à mesure de l'avancement dans la démarche.

Recommandé	Construire un glossaire
Il est RECOMMANDÉ de définir et répertorier, dans un glossaire, tous les termes utilisés.	

Cette démarche générique comprend quatre phases :

- Phase 1 : modéliser les processus collaboratifs, y compris les acteurs impliqués et les échanges,
- Phase 2 : modéliser les classes d'objets impliquées dans l'échange,
- Phase 3 : modéliser les informations échangées,
- Phase 4 : décrire les formats d'échanges.

Phase 1 : modéliser les processus collaboratifs

Cette modélisation sert à décrire les processus collaboratifs, les acteurs impliqués et les échanges entre ces acteurs.

Recommandé

Modéliser les processus collaboratifs

Il est RECOMMANDÉ de modéliser les processus collaboratifs à mettre en œuvre pour échanger l'information.

Les processus collaboratifs peuvent être formalisés textuellement et graphiquement par des diagrammes de processus.

Les diagrammes de cas d'utilisation (Figure 7) sont appropriés pour identifier les processus collaboratifs et les acteurs impliqués ou parties prenantes.

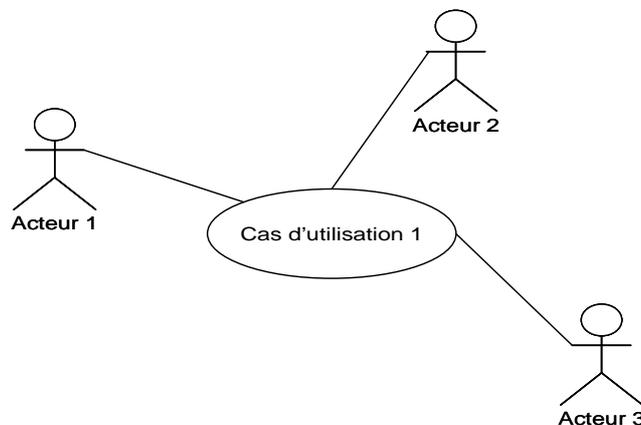


Figure 7 Exemple de diagramme de cas d'utilisation

Les diagrammes de description de processus BPMN (*Business Process Modeling Notation*) ou les diagrammes d'activités dont un exemple est présenté en figure 8, permettent de décrire un processus collaboratif. Ces diagrammes montrent pour chaque acteur, l'enchaînement des activités émettant ou recevant un échange d'informations.

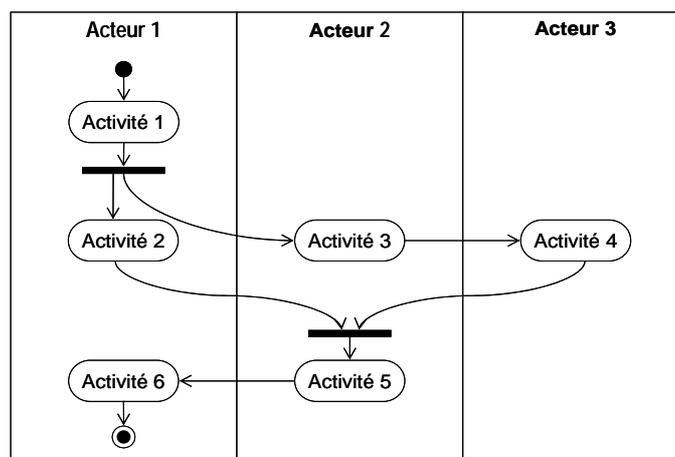


Figure 8 : Exemple de diagramme d'activités

Phase 2 : modéliser les classes d'objets impliquées dans l'échange

La phase 1 a permis d'identifier et de décrire les échanges entre les acteurs. Il s'agit maintenant d'identifier et de définir les informations que ces échanges transportent. La formalisation de ces informations en classes d'objets permet de bien répondre à cette exigence. Les spécifications, représentées par les modèles conceptuels, essaient de refléter au maximum la terminologie de contexte métier.

Différents langages graphiques et textuels permettent de décrire les classes à ce niveau, comme par exemple un modèle entité-relation ou un modèle de classes UML (voir Figure 9).

Recommandé Modéliser les classes d'objets impliquées dans l'échange

Il est RECOMMANDÉ de modéliser les informations de l'échange sous la forme de classes d'objets.

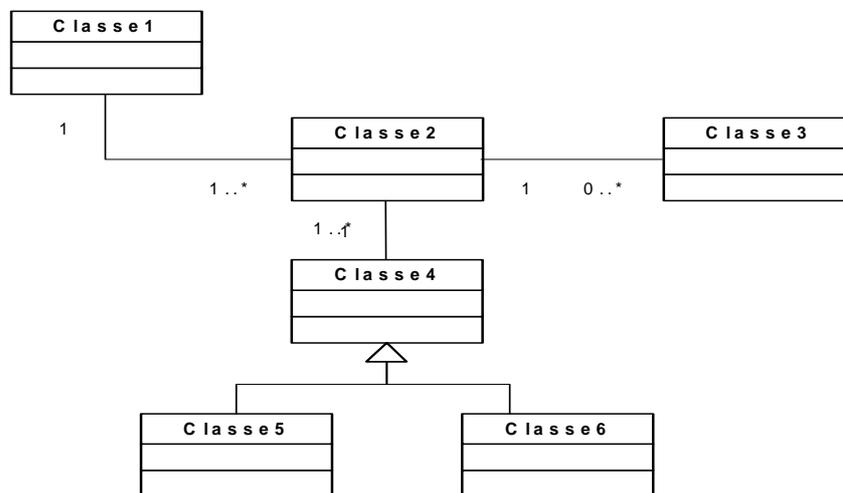


Figure 9 : Diagramme de classes UML

Phase 3 : modéliser les informations échangées

Cette phase consiste à :

- dériver le modèle d'informations échangées à partir du modèle des classes d'objets impliquées dans l'échange défini en phase 2,
- réutiliser, en les adaptant au contexte par des règles de nommage, des composants sémantiques préalablement mutualisés ou normalisés.

Ce modèle, neutre par rapport à la syntaxe, c'est-à-dire au format de l'échange, décrit pour chacune des informations de l'échange :

- sa définition,
- son nom, déduit de sa définition,
- son type, comme par exemple un code, un texte, une image, un montant, etc.
- et si son type est un code, la liste de codes dont il est issu comme par exemple, la liste des codes ISO 3166 des pays ou la NAF (Nomenclature des Activités Françaises).

Recommandé

Modéliser les informations échangées

Il est RECOMMANDÉ de modéliser les informations échangées.

Phase 4 : décrire les formats d'échanges

Cette phase constitue l'articulation entre le niveau sémantique et le niveau syntaxique. Elle est présentée au niveau sémantique afin de fluidifier le propos.

Elle consiste à traduire le modèle d'informations échangées en un message. Ce message contient l'ensemble des données à échanger. Il est bâti selon une syntaxe (ou format d'échange) commune aux parties prenantes de l'échange, par exemple un message XML.

Lors de l'échange, il est possible d'associer au message une description de ses données. Lorsque cette description n'est pas transmise avec le message, elle peut être précisée dans une convention entre les parties prenantes.

Recommandé Générer le format d'échange à partir du modèle d'informations échangées

Il est RECOMMANDÉ de générer le format d'échange à partir du modèle d'informations échangées.

Vue synthétique de la démarche générique de conception des échanges

Le tableau présenté en Figure 10 associe les modèles et les règles décrites aux phases de la démarche générique de conception des échanges.

Démarche générique	Modèles et règles
Modéliser les processus collaboratifs	Modèles de processus
Modéliser les classes d'objets impliquées dans l'échange	Modèles de classes d'objets
Modéliser les informations échangées	Règles de dérivation des diagrammes de classes en modèles d'informations Réutilisation en les adaptant au contexte des composants sémantiques préalablement mutualisés ou normalisés
Décrire les formats d'échanges	Traduction des modèles d'informations échangées dans une syntaxe commune aux parties prenantes

Figure 10 : Démarche générique de conception des échanges (synthèse)

2.3. Méthodes de spécification et langages

2.3.1. Méthodes de spécification

A la démarche générique de conception des échanges présentée ci-dessus, il est possible d'associer des méthodes de spécifications. Ces méthodes peuvent soit porter spécifiquement sur les échanges comme les méthodes UN/CEFACT, soit inclure la réflexion sur les échanges dans une spécification plus globale des SI comme la méthode Praxeme.

2.3.1.1. La méthode Praxeme

Praxeme est une méthode de modélisation d'entreprise et de conception de SI. Elle considère l'aspect sémantique d'un système comme le plus fondamental de son cadre architectural. Ce cadre est appelé « topologie du système », voir Figure 11.

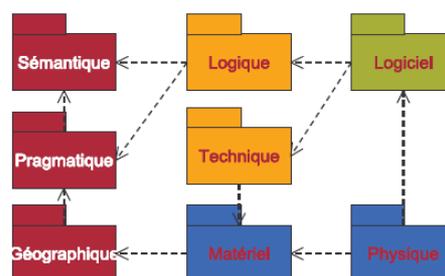


Figure 11 : Topologie du système Praxeme

La méthode Praxeme est une méthode dite « d'entreprise », car elle est destinée à couvrir tous les aspects d'une « entreprise » (terme employé pour désigner de manière générale toute organisation), depuis sa stratégie jusqu'au développement de son SI. Elle couvre notamment au travers de son point de vue dit « sémantique » la modélisation des concepts manipulés par l'entreprise et au travers de son point de vue dit « pragmatique » la modélisation des processus d'entreprise.

[Praxeme](#) est une méthode publique. Elle est basée sur les standards UML et MDA (*Model Driven Architecture*) de l'OMG (*Object Management Group*). Les éléments de la méthode ainsi que les modèles d'aspects ou de domaines rencontrés de manière récurrente dans les SI sont publiés en français et en anglais.

Praxeme n'est pas spécifiquement destinée aux échanges, ni à l'interopérabilité. Elle ne couvre qu'en partie les étapes de la démarche générique de description des échanges. Mais elle est citée pour sa capacité à répondre au besoin de modélisation des processus, des acteurs et des objets métier.

2.3.1.2. Les méthodes de l'UN/CEFACT

Avec l'aide de nombreuses institutions et en s'appuyant sur des spécifications méthodologiques de l'UN/CEFACT, un guide dédié à la dématérialisation des échanges pour améliorer l'interopérabilité des SI a été élaboré. Appelé actuellement "[Guide UML-XML](#)", un nom reflétant mieux son objet lui sera attribué lors de sa prochaine mise à jour.

Le but de ce guide est d'aider les maîtrises d'ouvrage et maîtrises d'œuvre des projets à modéliser les échanges et générer les formats techniques des données échangées. Sa lecture requiert seulement une connaissance de base des concepts UML, de la modélisation et du langage XML. Une connaissance approfondie des spécifications techniques sous-jacentes n'est pas indispensable.

Ce guide regroupe quatre approches UMM (*UN/CEFACT Modeling Methodology*), dérivation du diagramme de classes, CCTS (*Core Component Technical Specifications*) et XML NDR (*XML Naming and Design Rules*).

L'approche UMM définit les modèles UML et la documentation associée à produire pour modéliser les exigences « métier » d'un processus collaboratif. Elle sert à décrire les échanges, concevoir les modèles d'informations sur lesquels les partenaires doivent s'accorder afin de collaborer. Elle correspond aux deux premières phases de la démarche générique (voir tableau en Figure 12).

L'approche Dérivation des diagrammes de classes permet de transformer la structure d'un modèle conceptuel en une structure hiérarchique adaptée à l'échange d'informations.

L'approche CCTS décrit une méthode pour identifier (notamment à partir d'une structure hiérarchique adaptée à l'échange d'informations) un ensemble commun de « briques » sémantiques à réutiliser en les adaptant au contexte.

La spécification CCTS est une norme [ISO](#) (comité technique TC154: Processes, data elements and documents in commerce, industry and administration).

L'approche Dérivation des diagrammes de classes et la CCTS correspondent à la troisième phase de la démarche générique (voir tableau en Figure 12).

L'approche XML NDR définit des règles de nommage et de conception des messages XML (données et schémas). Elle a pour objectif de transformer un modèle de données échangées, description sémantique de l'échange, en un message dont la syntaxe puisse être reconnue par les parties prenantes de l'échange. Le schéma généré est un schéma XML UN/CEFACT. Cette approche correspond à la quatrième phase de la démarche générique (voir tableau en Figure 12).

Le tableau en Figure 12, présente les méthodes de l'UN/CEFACT couvrant les phases de la démarche générique.

Démarche générique	Modèles et règles	Méthodes UN/CEFACT
Modéliser les processus collaboratifs	Modèles de processus	UMM
Modéliser les classes d'objets impliquées dans l'échange	Modèles de classes d'objets	
Modéliser les informations échangées	Règles de dérivation des diagrammes de classes en modèles d'informations Réutilisation, en les adaptant au contexte des composants sémantiques préalablement mutualisés ou normalisés	CCTS
Décrire les formats d'échangés	Traduction des modèles d'informations échangées dans une syntaxe commune aux parties prenantes	XML NDR

Figure 12 : Couverture de la démarche générique par les méthodes de l'UN/CEFACT

2.3.2. Des langages pour décrire les échanges

Ce chapitre décrit les langages de spécification pouvant être utilisés pour décrire les échanges.

2.3.2.1. Le langage UML

UML (*Unified Modeling Language*), est un langage de modélisation graphique permettant de spécifier, visualiser et documenter les systèmes d'information.

UML est issu des notations de modélisation proposées par les méthodes objet les plus reconnues. Personnalisable par ses notations et supporté par une offre d'outils importante, il est devenu un standard de fait en informatique. Sa version standard initiale 1.1 fut adoptée par l'OMG en novembre 1997. L'ISO a adopté sa version 1.4.2 comme standard (ISO/IEC 19501:2005) en 2005. Actuellement (février 2009) la version 2.1.2 d'UML est le résultat du travail et des recommandations émanant à la fois des experts en méthodologie et des praticiens du monde entier.

UML permet de modéliser, entre autres:

- les acteurs et processus collaboratifs entre organismes ou systèmes, à l'aide de diagrammes de cas d'utilisation,
- les processus collaboratifs et leurs échanges, à l'aide de diagrammes d'activités, diagrammes d'interactions (collaborations et séquences) et diagrammes d'états-transitions,
- les informations échangées, à l'aide de diagrammes de classes,
- les systèmes composants et leurs interfaces, à l'aide de diagrammes de composants.

La modélisation en UML est facilitée par l'utilisation d'un outil logiciel de modélisation supportant cette notation. Il est souhaitable que cet outil supporte à la fois la dernière version d'UML (ou au moins la version 1.4.2 qui est également reconnue comme un standard ISO) et la dernière version du standard d'échange de métadonnées XMI. XMI permet d'exporter ou d'importer des spécifications écrites en UML vers ou depuis d'autres outils logiciels de modélisation UML.

2.3.2.2. La notation BPMN

BPMN (*Business Process Modeling Notation*), notation de modélisation des processus (métier), est une initiative du BPMI (*Business Process Management Initiative*) maintenue au sein de l'OMG depuis 2005.

BPMN permet de modéliser les acteurs et les processus. Le langage est graphique et articulé notamment autour des concepts d'activité, d'événement, de flots de contrôle et de flots de messages.

La notation BPMN est supportée par de nombreux outils du marché.

Recommandé	UML / BPMN	ISO/OMG	
Il est RECOMMANDÉ d'utiliser les langages de modélisation UML et/ou BPMN pour représenter et modéliser les processus collaboratifs.			
Il est RECOMMANDÉ d'utiliser le langage de modélisation UML pour modéliser les autres concepts de l'échange (les acteurs, les objets).			

2.3.2.3. Le langage OCL

Pour compléter la modélisation en UML, il est parfois approprié d'utiliser le langage OCL. OCL (*Object Constraint Language*) permet notamment d'exprimer des assertions (typiquement des conditions invariantes), spécifier des opérations ou des actions modifiant l'état des objets d'un diagramme de classes UML. [OCL](#) est un standard de l'OMG.

2.3.2.4. Des langages pour décrire des messages

2.3.2.4.1. Le langage XML

Les modèles d'informations échangées peuvent être traduits en différents langages, notamment le langage XML. Dans un document XML, il est possible de définir à la fois les données et la structure de ce document. Cette structure, appelée « schéma » peut être décrite dans un langage de définition de schéma.

2.3.2.4.2. La syntaxe XSD

La syntaxe XSD (*XML Schema Definition*) permet de décrire la structure et le contenu d'un document XML et de vérifier la validité des données qui le composent.

Recommandé	XSD	W3C	
Il est RECOMMANDÉ d'utiliser des schémas XSD pour décrire le contenu et la structure d'un document XML.			

Dans la pratique, il existe de nombreuses constructions de schémas XSD comme :

- les schémas standards de l'UN/CEFACT,
- les schémas liés à des pratiques sectorielles comme le schéma HL7 dans le domaine de la santé,
- les schémas XSD *ad hoc* non standards ou encore appelés "propriétaires".

Des partenaires peuvent avoir spécifié un modèle d'informations commun pour leur échange et avoir recours à des techniques de construction différentes de leurs documents XML (schémas XSD construits différemment) ou encore utiliser des syntaxes différentes.

Dans ce cas, ils ont recours à une technique de transformation de document XML en utilisant XSLT (*Extensible Stylesheet Language Transformations*).

Dans certains cas, cette solution peut se révéler pratique à court terme. Pour des raisons de maintenance et d'évolutivité, il est cependant recommandé aux parties prenantes de réutiliser les standards existants et de s'entendre sur une même construction syntaxique.

2.3.2.4.3. Autres syntaxes

Il existe d'autres syntaxes non XML permettant l'échange de données, dont les deux suivantes antérieures à XML sont très largement répandues:

- UN/EDIFACT
 Sous l'autorité des Nations Unies, EDIFACT (*United Nations/Electronic Data Interchange For Administration, Commerce and Transport*) repose sur une syntaxe (norme ISO 9735), des répertoires de données et des guides pour les échanges de données structurées entre systèmes d'information indépendants ;
- ASC X12
 L'ASC X12 (*Standards Committee X12*) accrédité par l'ANSI (*American National Standards Institute*) a également défini de nombreux standards liés à l'échange de documents électroniques ; il existe de nombreuses tables de correspondance entre les échanges X12 et EDIFACT.

2.3.2.5. Synthèse des langages et des syntaxes à utiliser

Le tableau en Figure 13, présente les modèles ou règles ainsi que les notations ou langages couvrant les phases de la démarche générique.

Démarche générique	Modèles ou règles	Notations ou langages
Modéliser les processus collaboratifs	Modèles de processus	Diagramme de cas d'utilisation UML Diagramme d'activités UML Diagramme d'états UML Diagramme d'interactions UML Diagramme de processus BPMN
Modéliser les classes d'objets impliquées dans l'échange	Modèles de classes d'objets	Diagramme de classes UML OCL
Modéliser les informations échangées	Règles de dérivation des diagrammes de classes en modèles d'informations Réutilisation, en les adaptant au contexte, des composants sémantiques préalablement mutualisés ou normalisés	
Décrire les formats d'échangés	Traduction des modèles d'informations échangés dans une syntaxe commune aux parties prenantes	Constructions de définitions de schémas à partir du langage XML: <ul style="list-style-type: none"> ○ Schémas UN/CEFACT ○ Schémas sectoriels (HL7,...) ○ Schémas ad hoc, ○ Etc. EDIFACT ANSI ASC X12 Etc.

Figure 13 : Les modèles ou règles ainsi que les notations ou langages pour décrire les échanges

2.4. Réutilisation des ressources sémantiques

Assurer l'interopérabilité sémantique suppose des efforts de mutualisation de systèmes communs d'identification, de sorte qu'un même objet, une même information ou une même valeur puisse toujours correspondre à un même concept ou une même caractéristique. Cela peut être le cas, par exemple, du code identifiant une commune ou de la situation familiale d'une personne.

Cette interopérabilité sémantique est fondée sur la mutualisation de ressources sémantiques constituées notamment de modèles décrivant la structure de l'information, de répertoires d'identification ou d'immatriculation, de bases de données de référence, de simples listes de valeurs ou de nomenclatures.

A titre d'exemple, la figure 14 présente un extrait de la description de la classe générique Personne de la bibliothèque MDC (Modèle de Données Communes), voir 2.4.1.5. DGME.

<p>Classe Personne Un individu titulaire de droits et d'obligations caractérisé par une identité civile constituée de l'ensemble des éléments d'état civil</p> <p>Attributs :</p> <ul style="list-style-type: none"> • Identifiant Identifiant unique pérenne de la personne. • Nom Famille Nom de famille selon les dispositions de la loi n° 2002-304 du 4 mars 2002 relative au nom de famille: • Prénom Usuel La notion de prénom usuel est prévue par l'article 57 du code civil qui définit le contenu de l'acte de naissance. Ministère de la Justice: " Tout prénom inscrit dans l'acte de naissance peut être choisi comme prénom usuel". Le prénom usuel est donc celui des prénoms indiqués dans l'acte de naissance dont il est fait usage dans la vie courante. • Sexe Sexe de la personne. Liste de codes associée provenant de la norme ISO 5218 1977 (E) : 1 = Masculin ; 2 = Féminin ; 9 = Indéterminé ou non spécifié • Situation Familiale Situation familiale de la personne. Liste de codes associée : 01 : célibataire ; 02 : marié ; 03 : divorcé ; 04 : séparé ; 05 : veuf, veuve ; 06 : vie maritale ; 07 : PACS ; 90 : non connue
--

Figure 14 : Extrait de la classe générique Personne du MDC

Ces ressources peuvent être centralisées et mutualisées par des institutions telles que des administrations ou des organismes de normalisation. Elles peuvent être très générales et utiles à l'ensemble des échanges de l'administration ou bien très centrées sur un secteur donné.

Un premier ensemble de ressources est constitué par les référentiels nationaux et les listes de codes et nomenclatures officielles.

2.4.1. Ressources communes aux échanges

Les ressources citées dans ce document ne sont pas exhaustives; celles des institutions suivantes sont données à titre d'exemple.

2.4.1.1. Insee

L'[Insee](#) gère :

- les principaux répertoires dans le domaine économique, social et spatial, notamment les répertoires de données RNIP (Répertoire National d'Identification des Personnes Physiques), RNIAM (Répertoire National Inter-régimes des bénéficiaires de l'Assurance Maladie) ou SIRENE (Système Informatisé du Répertoire National des Entreprises et des Etablissements) et les principales nomenclatures françaises telles que : COG (Code Officiel Géographique), APE (Activités principales des Entreprises et établissements) et NAF (Nomenclature des Activités Françaises), etc.
- Les définitions des concepts les plus souvent utilisés dans les études;
- les schémas XML permettant de représenter des données d'identification et de classification.

2.4.1.2. Eurostat

Eurostat met à disposition un serveur de nomenclatures appelé [RAMON](#). Diverses listes de codes et nomenclatures concernant les biens, les activités économiques et les statistiques au niveau européen y sont accessibles.

2.4.1.3. ISO

L'ISO normalise notamment des types de données comme la représentation de la date et de l'heure (ISO 8601), des listes de codes comme la liste des noms et codes de pays (ISO 3166), des codes pour la représentation des noms de langues (ISO 639-1) ou encore des codes de représentation des sexes humains (ISO 5218).

Les [ressources ISO](#) sont généralement payantes. Néanmoins, certaines [ressources ISO](#) sont disponibles gratuitement.

2.4.1.4. UN/CEFACT

L'[UN/CEFACT](#) met à disposition un ensemble important de recommandations (normes et standards) dont les ressources suivantes :

- Les spécifications fonctionnelles basées sur les modèles UML (BRS – *Business Requirement Specifications*), les spécifications techniques basées sur les diagrammes de classes hiérarchiques (RSM - *Requirement Specification Mapping*) et les schémas XSD des échanges de données standardisés;
- La bibliothèque des composants communs (CCL - *Core Component Library*) contenant à la fois des composants génériques neutres à contextualiser (CC - *Core components*) et des composants contextualisés aux échanges (BIEs - *Business Information Entities*) et les descriptions de types de données;
- Les répertoires EDIFACT;
- Des listes de codes et des nomenclatures.

2.4.1.5. DGME

La DGME, en collaboration avec l'ensemble des ministères, développe la ressource [MDC](#) (Modèle de Données Communes). Le MDC définit plusieurs dizaines de concepts, sous la forme de classes d'objets, communs à toutes les administrations comme, par exemple, "Personne", "Organisation" ou "Adresse". Ces concepts peuvent être vus comme des

constantes intersectorielles susceptibles d'être réutilisées dans de nombreux formulaires et procédures administratives.

Présenté sous forme d'un dictionnaire de structures de données échangeables, le MDC doit permettre l'élaboration et la diffusion d'une terminologie commune aux SI de l'administration. Le MDC respecte les normes et standards de l'UN/CEFACT. Il a pour origine la bibliothèque de composants communs de l'UN/CEFACT (UN/CEFACT CCL). Ces composants sont traduits au fil de l'eau et adaptés au contexte de l'administration française.

Des acteurs de différents secteurs professionnels de l'administration contribuent à l'élaboration commune et la mise à jour régulière du MDC.

Le MDC s'adresse aux maîtrises d'ouvrage et aux maîtrises d'œuvre en charge de projets liés aux échanges de données. La réutilisation des classes d'objets du MDC permet de réduire les ambiguïtés sémantiques sur les données échangées. Les modèles, définitions et nommages de données du MDC sont destinés à faciliter l'élaboration des schémas XML d'échanges entre SI.

Recommandé

Réutiliser les ressources sémantiques

Il est RECOMMANDÉ lors de la conception des échanges de réutiliser des ressources sémantiques existantes.

2.4.1.6. SEMIC.EU

[SEMIC.EU](#) (*Semantic Interoperability Centre Europe*) est un service européen fourni par la Commission européenne dans le cadre du programme IDABC (*Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens*) qui valorise les ressources sémantiques des administrations. Ce répertoire permet aux administrations européennes d'y déposer des méthodes et outils ainsi que des concepts, des modèles de données et des listes de codes afin de les rendre visibles aux autres administrations pour réutilisation. Cette mise en commun permet de favoriser l'interopérabilité sémantique.

Une synthèse des ressources

Générales ou sectorielles, ces ressources sont de nature différente. Le tableau en Figure 15 présente les types de ressources réutilisables à chaque phase de la démarche générique.

Démarche générique	Types de ressources réutilisables	Description
Modéliser les processus collaboratifs	Diagrammes d'activités	Des modèles de processus collaboratifs et de classes d'objets
Modéliser les classes d'objets impliquées dans l'échange	Diagramme de classes	
Modéliser les données échangées	Diagrammes de classes	Des diagrammes de classes des informations échangées
	Classes d'objets mutualisées	Classes d'objets avec leurs attributs
	Types de données	Types de données associées aux attributs des classes d'objets (ex.: une date, un montant, etc.)
	Listes de codes, nomenclatures	Des listes de valeurs associées une donnée (exemple : code NAF)
Décrire les formats d'échangés	XSD données	Des schémas XML reprenant la description des données (exemple : l'adresse client)
	XSD valeurs	Des schémas XML reprenant la liste des valeurs possibles associée une donnée (exemple : la liste des codes pays)

Figure 15 : Les types de ressources réutilisables

Précisions sur les listes énumérées

Une liste énumérée désigne une liste finie de codes (numériques, alphanumériques, mnémoniques) faisant autorité et servant de référence à une discipline donnée.

Les codes sont utilisés pour mémoriser et transmettre l'information décrite sans ambiguïté lorsque la liste est identifiée.

On distingue deux types de listes de codes énumérées :

- la liste de valeurs : elle se présente sous forme d'une liste de codes auxquels correspondent des libellés (exemple : la liste des codes pays) ;
- la nomenclature : elle se présente sous forme d'une liste de codes induisant une classification sous-jacente, une taxonomie préétablie; par exemple, dans la nomenclature combinée servant à identifier les produits, le code "0603 11 00" désigne les "Roses et leurs boutons, frais, coupés, pour bouquets ou pour ornements" ; dans ce code, le premier groupe de deux caractères "06" désigne les "plantes vivantes et produits de la floriculture", le second groupe de deux caractères "03" désigne le groupe des "fleurs et boutons de fleurs, coupés, pour bouquets ou

pour ornements, frais, séchés, blanchis, teints, imprégnés ou autrement préparés" et le dernier groupe "11 00" désigne les "roses".

Précisions sur les conflits entre listes énumérées

Une des principales difficultés en matière d'interopérabilité sémantique provient de l'existence de multiples listes énumérées concurrentes locales voire spécifiques à des applications.

Pour chaque donnée ou attribut correspondant à une notion de type énumérable, la liste de codes qui sert à donner une « valeur normalisée » à l'information à échanger est :

- soit une liste de codes unique, imposée aux parties prenantes en amont des échanges,
- soit une liste de codes déclarée commune pour l'échange; dans ce cas, chacune des parties prenantes conserve en interne sa propre liste de codes et prend en charge, en entrée et sortie, les transcodages ou transpositions dans le langage commun de toutes les valeurs affectées aux données.

Les principes de classement et de construction des codifications ne sont pas toujours explicites, documentés ou connus. C'est alors au niveau des tables de transcodage qu'apparaissent les difficultés principales. Ces tables doivent être conçues pour accepter le niveau le plus fin d'information. Ce travail est souvent fastidieux et des suites d'approximations génèrent souvent une perte d'information.

La préoccupation d'interopérabilité suggère de recourir à des listes de codes bien établies et d'usage courant.

2.4.2. Ressources pour l'archivage

2.4.2.1. La nécessité de l'archivage numérique

Le cycle de vie

Tout système d'information, dès sa mise en œuvre, doit intégrer les problématiques liées au cycle de vie de l'information, notamment aux durées de conservation des documents et des données. Cette démarche inclut :

- la mise en œuvre d'un archivage intermédiaire, si les durées de conservation sont longues,
- l'élimination réglementaire, si la conservation d'un document n'est pas justifiée,
- le versement dans les services publics d'archives.

Il est nécessaire que les modalités mises en place permettent de garantir que chaque document archivé reste lisible et intelligible, imputable à un auteur identifié, fiable et intègre jusqu'au terme du délai durant lequel des droits y afférant peuvent exister.

Recommandé

Gérer le cycle de vie des informations

Afin de gérer le cycle de vie de l'information, il est RECOMMANDÉ que tout système d'information mette en œuvre les fonctionnalités liées aux durées de conservation des documents/données.

L'interopérabilité

L'archivage numérique nécessite une interopérabilité dans le temps des systèmes de collecte, conservation et consultation.

D'un point de vue technique, cette interopérabilité repose sur la prise en compte des caractéristiques des supports physiques permettant la conservation des données, leur surveillance et leur migration sur d'autres supports. Elle concerne aussi la réplication des données/documents sur des sites distants. Les recommandations couvrant ces aspects sont disponibles sur le site de la [DAF](#) (Direction des Archives de France).

D'un point de vue syntaxique, cette interopérabilité repose sur la prise en compte des caractéristiques de formats de documents/données permettant la conservation des données. Les documents numériques doivent être enregistrés sur des formats pérennes, si possible, dès leur production. A défaut, ils devront être convertis dans un format pérenne à des fins de conservation.

D'un point de vue sémantique, cette interopérabilité implique de prendre en compte:

- le contexte de l'archivage,
- le processus d'archivage,
- le sens et la structuration des informations à archiver.

2.4.2.2. Le contexte de l'archivage

Cadre législatif

Les obligations légales en matière de gestion fiscale, comptable ou sociale imposent souvent aux administrations et aux entreprises de conserver des documents sur de longues périodes.

Le code du patrimoine définit les archives comme « l'ensemble des documents, quels que soient leur date, leur lieu de conservation, leur forme et leur support, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité » (article L. 211-1).

Les archives publiques sont « les documents qui procèdent de l'activité de l'État, des collectivités territoriales... » (article L 211-4).

Les règles de gestion des documents d'archives publiques au long de leur cycle de vie sont définies par le décret n° 79-1037 du 3 décembre 1979 modifié par le décret n° 2006-1828 du 23 décembre 2006.

Pour plus d'informations sur le cadre législatif régissant l'archivage, diverses sources peuvent être consultées :

- le [code du patrimoine](#),
- les [circulaires de la DAF](#),
- Les [recommandations de la CNIL](#),
- Une synthèse des [enjeux juridiques](#).

Politique d'archivage et système d'archivage électronique (SAE)

La politique d'archivage définit les exigences minimales, en termes juridiques, fonctionnels, opérationnels, techniques et de sécurité, qu'une autorité d'archivage doit respecter afin que l'archivage électronique mis en place soit considéré comme fiable.

Le document « [Politique et pratique d'archivage](#) » décrit les concepts de politique d'archivage et de déclaration des pratiques d'archivage.

Le « [records management](#) » définit l'organisation et la gestion de l'information notamment la création, la réception, la conservation, l'utilisation et le sort final des documents d'archives. Il décrit aussi les méthodes de fixation et de préservation de la preuve liées à la forme des documents.

[Moreq2](#) est un document de référence en matière d'organisation de l'archivage. Fondé sur la norme ISO 15489, le modèle définit des exigences génériques pour un système électronique de gestion des archives et des logiciels de « records management » en particulier.

Pour mettre en œuvre un système d'archivage électronique, [OAIS](#) (Modèle de référence pour un système ouvert d'archivage, basé sur la norme ISO 14721) définit un vocabulaire et un ensemble de concepts permettant d'appréhender de façon globale et complète, la question de l'archivage à long terme des données sous forme numérique.

Recommandé

Mettre en œuvre un système d'archivage électronique

Pour mettre en œuvre un système d'archivage électronique, il est RECOMMANDÉ de se conformer au modèle OAIS et de définir une organisation et une politique de l'archivage.

2.4.2.3. Le processus d'archivage

Le [SEDA](#) (Standard d'Echange de Données pour l'Archivage) vise à faciliter l'interopérabilité entre le système d'information d'un service d'archives et les systèmes d'information de ses partenaires (producteurs, utilisateurs...).

Il définit la forme du dialogue ainsi que la forme des messages échangés pour les cinq principaux cas d'utilisation d'archivage - le transfert, la communication, la modification d'archives, l'élimination et la restitution.

Le standard SEDA permet de décrire la structure organisationnelle des contenus de données échangés (comme un bordereau de versement par exemple). Il est générique et adaptable à tous types de documents et de données, électroniques ou papier. Aussi, lors de la prise en compte d'un processus dans la chaîne de l'archivage, un profil d'archivage doit être établi pour préciser les règles de description spécifiques aux types de documents ou données versés.

Recommandé	SEDA	DAF	
<p>Pour mettre en place un processus d'archivage, il est RECOMMANDÉ que les services publics d'archives et leurs partenaires se réfèrent au « Standard d'Echanges de Données pour l'Archivage ».</p>			

2.4.2.4. Le sens et la structuration de l'information archivée

Un document numérique archivé est accessible grâce à la description de son contenu. Les données servant à définir ou décrire une autre donnée, un document par exemple, sont appelées métadonnées. Il existe plusieurs types de métadonnées pour décrire un document numérique.

Les métadonnées descriptives sont les métadonnées qui permettent d'identifier, classifier, hiérarchiser l'information contenue dans l'objet numérique. Elles ont été normalisées et sont les suivantes:

- Pour les documents d'archives, les normes établies par l'ICA (Comité International des Archives) sont les normes ISAd(G) (*General International Standard on Archival Description*), ISAAR(CFP) (*International Standard Archival Authority Record for Corporate Bodies, Persons, and Families*), ISDF (*International Standard for Describing Functions*) et ISDIAH (*International Standard for Describing Institutions with Archival Holdings*). Elles sont consultables sur les sites de la [DAF](#) et de l'[ICA](#) ;
- Le [Dublin Core](#), devenu norme ISO 15836 en 2003, est un schéma générique et simple de métadonnées; il s'appuie sur des éléments de description formels (titre, auteur, éditeur), intellectuels (sujet, description, langue, etc.) et relatifs à la propriété intellectuelle ;

Les métadonnées de structure servent à décrire les liens entre des éléments qui ont du sens pour l'utilisateur (numéro de page, de plage audio, titre de chapitre, d'article, etc.) et le mode d'enregistrement des objets numériques (répertoire, support, etc.). Les formats de métadonnées METS (*Metadata Encoding and Transmission Standard*) ou XFDU (*XML Formatted Data Unit*) sont de bons exemples.

Les *métadonnées techniques* permettent d'identifier et de caractériser les formats de représentation de l'information ou formats de données. Le dictionnaire [PREMIS](#) est, dans ce domaine, un outil très précis. Il vise à établir, à partir du modèle OAIS, une liste des métadonnées gérées dans le processus de conservation numérique.

Les *métadonnées administratives* sont les métadonnées qui servent à gérer la vie de l'objet numérique. Elles regroupent les métadonnées de contexte, de provenance, d'intégrité et de gestion des droits ainsi que les métadonnées permettant l'identification univoque et pérenne des objets archivés.

Concernant ce type de métadonnées, le choix d'un type d'identifiant est stratégique. Cet identifiant doit résister à l'épreuve du temps, aux évolutions de classement intellectuel des contenus, aux changements d'organisation physique des données et être indépendant des systèmes et des organisations.

L'IPTC (*International Press Telecommunications Council*) est un consortium regroupant des entreprises et des organisations actives dans le monde de la presse. L'IPTC a défini un standard informatique pour le stockage des métadonnées descriptives (titre, auteur, etc.) et administratives (copyright, etc.) relatives aux images de presse, l'IPTC Core. Ce standard est utilisé en particulier dans les fichiers [JPEG](#) et [TIFF](#).

Plus généralement, on peut caractériser un document dès sa création et tout au long de son cycle de vie par son identifiant, un titre (intitulé), un statut (document de travail/document validé/document périmé), au moins une date (qui selon le contexte peut être une date de création du document, d'archivage,...), une classification (rattachement à un dossier/répertoire), sa durée de conservation, le producteur du document et le service auquel il appartient.

Recommandé

Caractériser un document par ses métadonnées

il est RECOMMANDE qu'un document soit caractérisé, dès sa création et tout au long de son cycle de vie, par au moins un identifiant, un titre, un statut, une date, une classification, une durée de conservation, un producteur et le service auquel il appartient.

3. Interopérabilité syntaxique

L'interopérabilité syntaxique concerne la façon dont sont codées et formatées les données. Dans le RGI, elle est divisée en deux domaines :

- Les formats élémentaires
Les formats élémentaires incluent les formats pour le son, la photo, l'image animée et le codage des caractères.
- Les formats composites
Les formats composites, agrégats de plusieurs objets incluent, par exemple, les documents bureautiques et les formats de compression de fichiers.

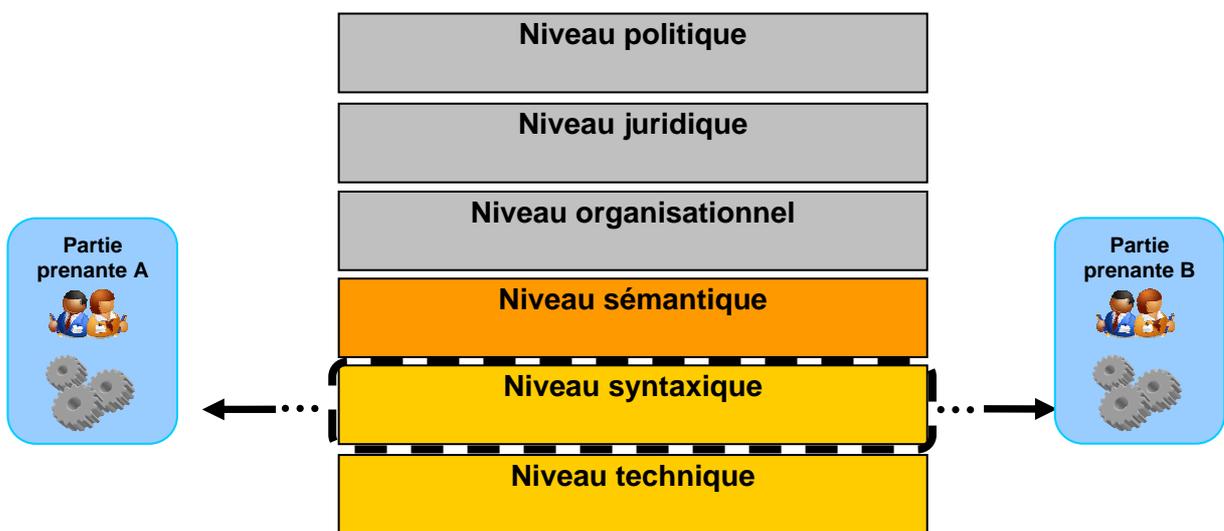


Figure 16 : Le niveau syntaxique traite du formatage de l'information

3.1. Formats élémentaires

3.1.1. Codage des caractères

UTF-8 (*UCS transformation format 8 bits*) est un format de codage de caractères défini pour les caractères UNICODE. C'est une extension du code ASCII utilisant le bit de poids fort. Chaque caractère est codé sur une suite de un à quatre octets.

Initialement, UTF-8 était décrit dans la RFC 3629 et défini dans le rapport technique 17 de la norme UNICODE. Il fait maintenant partie intégrante de la norme UNICODE dans son chapitre 3 « *Conformance* », approuvé également par l'ISO, l'IETF et la plupart des organismes de normalisation.

L'IETF requiert que UTF-8 soit supporté par les protocoles de communication du réseau Internet échangeant du texte. L'utilisation du format UTF-8 facilite à la fois la maintenance et l'accessibilité des sites Web. Les principaux navigateurs du marché prennent en charge la recommandation UTF-8 depuis 1998.

Recommandé	UTF-8	IETF	
Il est RECOMMANDÉ d'utiliser la transformation UTF-8 pour l'encodage des caractères.			

Même si le RGI ne s'applique qu'aux interfaces d'échanges, il est important de noter que le choix d'UTF-8 sur l'ensemble de la chaîne de traitement des caractères (couches de persistance, applicative, de présentation et d'échanges) permet d'améliorer l'interopérabilité.

3.1.2. Polices d'écriture

On appelle « police d'écriture » un ensemble de représentations visuelles de caractères d'une même famille. Cet ensemble regroupe tous les corps et graisses dont le style est coordonné afin de former un alphabet.

On appelle « fonte de caractères » un ensemble de représentations visuelles de caractères, d'une même famille, de même style (italique par exemple), corps et graisse.

Recommandé	Polices libres	W3C	
<p>Pour la mise forme électronique de données échangées, il est RECOMMANDÉ d'utiliser des polices de caractères supportées nativement par toutes les plates-formes.</p>			

Exemple de polices :

- Arial,
- Courier,
- Times New Roman,
- Verdana.

Remarque : les polices ne faisant pas l'objet de procédures de normalisation, des différences de rendu peuvent apparaître selon les implémentations et les outils.

3.1.3. Formats d'image

Les formats d'image ouverts et supportés nativement dans la majorité des navigateurs et systèmes informatiques sont les suivants :

- GIF (*Graphic Interchange Format*) : particulièrement adapté pour les images de 256 couleurs ou moins, pour les images nécessitant une couche de transparence et pour les animations simples ;
- PNG (*Portable Network Graphics*) : défini par la norme ISO 15948, il supporte 16 millions de couleurs, la transparence et peut également convenir pour des images photographiques ;
- JPEG (*Joint Photographic Experts Group*) : défini par la norme ISO 10918, il très utilisé pour la photographie numérique ; il permet un haut niveau de compression (de l'ordre de 1/40) qui convient particulièrement à la compression de photographies
- TIFF (*Tagged Image File Format*) : format de fichier graphique bitmap, adapté pour les images de tailles importantes et de haute qualité ;
- DNG (*Digital Negative*) : format dérivé de TIFF qui enregistre les signaux bruts des appareils photographiques.

Le choix du format utilisé dépend :

- De la qualité de l'image souhaitée,
- De la taille du fichier cible,
- Du type d'usage (affichage, impression, échange, conservation, etc.).

Les caractéristiques de l'image doivent être adaptées aux besoins du destinataire. Ainsi, une image de 256 couleurs avec une couche de transparence, peut utiliser les formats PNG-8 ou GIF, le choix final pouvant dépendre de la taille du fichier image.

Recommandé	Formats d'image
	Pour les images numériques, il est RECOMMANDÉ de choisir parmi les formats GIF, PNG, JPEG, TIFF ou DNG.

Remarque : afin de pouvoir modifier une image, les fichiers originaux de création de cette image doivent être conservés.

3.1.4. Formats de séquence sonore

MP3 est l'abréviation de *MPEG-1 Audio Layer 3*, la spécification sonore du format MPEG-1, du MPEG (*Moving Picture Experts Group*). MP3 (ISO 11172-3) est un algorithme de compression capable de réduire fortement la quantité de données nécessaires à la restitution d'un son monophonique ou stéréophonique. Pour l'oreille humaine, la perte de données due à la compression altère peu la qualité de l'enregistrement sonore.

Recommandé	MP3	ISO	
Il est RECOMMANDÉ d'utiliser le format MP3 pour l'échange, la diffusion et la conservation des séquences sonores de qualité ordinaire.			

En observation	Ogg- Vorbis	Xiph	
De conception moderne, l'algorithme de compression Vorbis, qui est encapsulé la plupart du temps dans le format ouvert Ogg, offre un son de bonne qualité et un excellent taux de compression. Malgré une adoption croissante, ce format est aujourd'hui moins utilisé que le format MP3.			

Le format WAV, basé sur le format RIFF (*Resource Interchange File Format*), permet de restituer des fichiers sonores sans perte de données .
 A l'origine, il est le format des fichiers sonores du système d'exploitation Windows. Il a été développé par les sociétés Microsoft et IBM. Il est maintenant élargi à d'autres plates-formes comme GNU/Linux par exemple. Le format WAV peut être utilisé avec un codage PCM (*Pulse Code Modulation*) c'est-à-dire sans compression, les fichiers résultants sont de haute qualité sonore mais volumineux. Le format [BWF](#), moins répandu à ce jour, permet d'associer des méta-données aux fichiers WAV.

Recommandé	WAV	IBM & Microsoft	
Il est RECOMMANDÉ d'utiliser le format WAV avec un codage PCM, pour l'échange, la diffusion et la conservation des séquences sonores de haute qualité.			

En observation	FLAC	Xiph	
FLAC est un format de compression audio sans perte. Il n'enlève aucune information du flux audio, tout en réduisant la taille des fichiers. Ses spécifications sont libres et il est disponible sur toutes les plateformes. Si sa maturité est croissante, il manque aujourd'hui d'adoption par le marché.			



Concernant les formats audio utilisés dans le cadre de la téléphonie sur IP, se reporter au chapitre [4.2.2.3 Codage de voix](#) et [4.2.2.5 Convergence des messageries](#)

3.1.5. Formats de séquence vidéo

MPEG-2 est la norme de seconde génération issue des travaux du Moving Picture Experts Group qui fait suite à MPEG-1.

La norme MPEG-2 (ISO 13818) définit les aspects compression de l'image et du son et le transport à travers des réseaux pour la télévision numérique. Cette norme de compression pour les images animées fonctionne sur toutes les plates-formes.

La norme ISO/IEC 13818-1 définit les aspects synchronisation, transport et stockage et les normes ISO/IEC 13818-2 et 3 définissent les aspects compression du signal.

Recommandé	MPEG-2	ISO	
Il est RECOMMANDÉ d'utiliser la norme MPEG-2 pour l'échange, la présentation et la conservation de séquences vidéo en basse définition.			

La norme MPEG-4 (ISO 14496) est une norme de compression pour les images animées, définie par le Moving Picture Expert Group de l'ISO. Elle a été publiée en 1998. MPEG-4 permet de gérer des flux pour l'accès à travers le réseau Internet. Elle permet aussi de gérer la vidéoconférence.

Le dernier niveau de la norme MPEG-4 est aussi nommé H.264 par l'UIT-T.

Recommandé	MPEG-4	ISO	
Il est RECOMMANDÉ d'utiliser la norme MPEG-4 pour l'échange, la présentation et la conservation de séquences vidéo en haute définition.			

Recommandé	MPEG-4 services audiovisuels	ISO	
Il est RECOMMANDÉ d'utiliser la norme MPEG-4 pour la mise en œuvre de services audiovisuels (vidéoconférence, visiophonie, etc.).			



Concernant les protocoles de diffusion vidéo, se reporter au thème 4.4.2.9 Diffusion vidéo en mode continu

3.1.6. Formats d'objet graphique en 2D

Les objets graphiques à deux dimensions sont des données administratives, sectorielles ou globales nécessitant l'utilisation de logiciels graphiques dédiés.

Les formats de graphiques vectoriels ne décrivent pas quelles proportions de couleurs possèdent un pixel de l'image, mais ils décrivent des objets. Cette forme de graphique est idéale pour le web : les données de description d'objets graphiques vectoriels étant en général plus légères que les graphiques orientés pixels. Ces formats sont appropriés au dessin industriel, aux illustrations et à toutes sortes de techniques graphiques.

Deux standards normalisés sont conseillés :

- Le format CGM (*Computer Graphic Metafile*) est une norme pour l'échange et la conservation de données graphiques à deux dimensions ; CGM (ISO 8632) est le format adopté dans de nombreux secteurs industriels comme par exemple l'industrie aéronautique (ATA, AECMA), le secteur automobile (J2008), la défense (CALs), les télécommunications et la pétrochimie ;
La format WebCGM est un profil spécifique développé pour les applications web, il a été normalisé par l'OASIS et le W3C.
- Le format SVG (*Scalable Vector Graphic*) est une recommandation du consortium W3C. Il est basé sur le langage XML et permet la description d'objets graphiques vectoriels en deux dimensions. Il permet l'interactivité et l'exécution de scripts et d'animations. Il est indépendant de la plate-forme, documenté, ouvert et peut être utilisé librement. Il est préféré à CGM pour les données graphiques de haute qualité et la création artistique.

Le format SVG se distingue par les propriétés particulières suivantes :

- il est basé sur le langage XML,
- il soutient le schéma Xlink,
- il a la possibilité d'être agrandi ou basculé,
- il interface le langage SMIL.

Les versions les plus récentes des logiciels de graphiques vectoriels connus soutiennent le format SVG. Les principaux navigateurs peuvent afficher des graphiques SVG. Il existe des programmes d'affichage SVG téléchargeables librement, certains pouvant être installés comme module d'extension au navigateur.

Recommandé	SVG/CGM	W3C/ISO	 
<p>Il est RECOMMANDÉ d'utiliser le format SVG 1.1 pour la description d'objets graphiques vectoriels en deux dimensions. Dans le cadre d'applications industrielles, dans les secteurs de la défense, l'aéronautique, l'automobile ou l'énergie, il est possible d'utiliser le format CGM.</p>			

3.1.7. Formats d'objet et d'univers 3D

Afin de proposer des objets et des univers en 3D, les autorités administratives ont à leur disposition de multiples applications de modélisation. Un effort doit être entrepris pour normaliser le format de ces objets.

X3D (Extensible 3D) est un format de fichier graphique et multimédia orienté 3D. Il a été créé par le consortium Web3D dans le but de succéder à VRML 2.0. Ce format a été normalisé par l'ISO.

Le format X3D s'appuie sur une structuration de type graphe de scène et peut être exprimé à l'aide de trois syntaxes différentes, à savoir la syntaxe VRML classique, une syntaxe basée sur le langage XML et une version binaire.

Il existe à ce jour deux API pour les langages ECMAScript (norme ISO 19777 partie 1) et Java (norme ISO 19777 partie 2).

Recommandé	X3D	ISO	
Il est RECOMMANDÉ d'utiliser le format X3D pour la description d'objets et d'univers virtuels en 3 dimensions.			

3.1.8. Formats de dessin technique

DWG est le format de fichiers du logiciel AutoCAD de la société Autodesk, produit incontournable dans le monde du dessin technique.

Un consortium à but non lucratif, l'ODA (*Open Design Alliance*) a été créé afin de favoriser la standardisation des dessins techniques. Le but était d'assurer la pérennité du format DWG dans l'avenir, à travers le format DWGdirect, mais également du format DGN à travers DGNdirect. Quasiment tous les concurrents de la société Autodesk ont adhéré à cette initiative.

Recommandé	DWGdirect	ODA	
Il est RECOMMANDÉ d'utiliser le format DWGdirect, ou à défaut le format DWG, pour les échanges de dessins techniques en mode révisable (par exemple des plans devant être exploités, voire modifiés).			

Il faut également noter l'existence du format DWF (*Design Web Format*), de la société Autodesk, dédié à la publication et au partage de dessins, de plans et de modèles sur le Web. Il permet de visualiser et d'imprimer des croquis et des plans issus de l'environnement Autocad (donc au format DWG) mais sans posséder l'application de conception d'origine. Pour ouvrir ces fichiers, il est nécessaire d'installer préalablement un outil de visualisation téléchargeable librement. Le format DWF est plus compact que le format DWG, qualité indispensable pour un partage sur le Web.

Echange de dessins techniques en mode non révisable

Le format PDF 1.7, normalisé par l'ISO en juillet 2008 (ISO 32000-1) est une alternative au format DWF, pour l'échange de fichiers de dessins techniques en mode non révisable. Il s'agit de dessins qui n'ont pas vocation à être modifiés par celui qui les reçoit.

Dans le cadre de la dématérialisation des appels d'offres, les formats PDF et DWF sont très utilisés pour la diffusion des plans. En effet, les plans inclus dans un dossier d'appel d'offres sont rendus publics, d'où un risque à les publier sous un format modifiable.

Dans le même esprit, le format PDF permet d'apporter un premier niveau de protection en limitant la copie illicite ou le plagia de plans ou de parties de plans.

Recommandé	PDF	ISO	
Il est RECOMMANDÉ d'utiliser le format PDF 1.7, ou à défaut le format DWF, pour les échanges de dessins techniques (par exemple des plans) en mode non révisable.			



Pour plus d'information sur PDF, se reporter aux chapitres 3.2.2 *Echange de documents bureautiques non révisables*, 3.2.3 *Archivage de documents bureautiques non révisables statiques*, 3.2.4 *Conservation des documents bureautiques dynamiques*, 3.2.5 *Echange de données numériques d'impression*

3.1.9. Exportation de bases de données

Il n'existe pas de standard de format élémentaire permettant d'échanger une exportation de base de données.

Plusieurs formats sont acceptables (XML, CSV), cependant aucun n'est autoporteur. Les fichiers produits doivent donc être accompagnés de documents précisant la structure et le contenu du fichier ainsi que le jeu de caractères utilisé.

Recommandé	XML / CSV	W3C	
Il est RECOMMANDÉ d'utiliser XML ou CSV pour l'exportation de tout ou partie d'une base de données.			

Remarque : XML n'est pas préconisé pour les volumétries importantes.

 Pour de plus amples informations sur les échanges XML se reporter au chapitre 3.2.6 *Echange de documents structurés*

3.2. Formats composites

Précisions terminologiques liées aux formats composites :

- Un document non structuré est un document ayant une structure libre, par exemple une page Web ;
- Un document semi-structuré est un document ayant une partie structurée et une partie dont la structure est libre. De nombreux formats de document, notamment ceux issus des logiciels bureautiques (traitement de texte, tableur, présentation, etc.), utilisent ce type d'organisation. Les logiciels de dessin technique, de CAO, de production industrielle entrent eux aussi dans cette catégorie ;
- Un document structuré est un document supportant un format dont chaque élément est parfaitement défini, par exemple une extraction de base de données ;
- Un document révisable est un document qui peut être modifié en utilisant des moyens ordinaires liés à la manipulation du format support de ce document ;
- Un document non révisable est un document qui ne peut pas être modifié en utilisant des moyens ordinaires liés à la manipulation du format support de ce document ;
- Un document bureautique dynamique est un document non révisable qui comprend des éléments tels que des scripts ou encore de l'audio ou de la vidéo.

3.2.1. Echange de documents bureautiques révisables

Les documents créés et manipulés par les suites bureautiques sont des documents semi-structurés. L'échange de documents bureautiques constitue un élément important du développement des échanges par voie électronique.

Recommandé	Langage XML	ISO
<p>Pour les échanges de documents bureautiques semi-structurés en mode révisable, il est RECOMMANDÉ d'utiliser un format de document basé sur le langage XML et dont les spécifications sont normalisées par l'ISO.</p>		

Deux formats bureautiques coexistent aujourd'hui sur le segment des documents bureautiques XML normalisés : ODF (*Open Document Format*) et OXML (*Office Open XML*).

ODF est un format bureautique basé sur le langage XML. La version 1.0 du format de document ouvert a été approuvée par l'organisation OASIS en mai 2005, puis par l'ISO en mai 2006.

Le format Office Open XML a été validé comme standard ECMA en décembre 2006. Depuis, les spécifications du format ont été amendées et sa normalisation par l'ISO est intervenue en novembre 2008 (ISO 29500).

En observation	ODF	OASIS	
<p>Des améliorations de la norme concernant l'accessibilité ont été apportées avec la version 1.1, approuvée par l'OASIS en octobre 2006. La majorité des implémentations du marché reprennent cette dernière version.</p> <p>La version ODF 1.2 est en cours d'élaboration et devrait être soumise à l'approbation OASIS et ISO en 2009.</p>			

En observation	Office Open XML	ISO	
<p>Le format Office Open XML est un format bureautique basé sur XML. Il supporte nativement une partie des formats binaires bureautiques existants. Il n'existe pas à ce jour d'implémentation de cette norme.</p>			

Les autorités administratives et les usagers peuvent choisir parmi plusieurs solutions bureautiques, ce qui rend critique l'interopérabilité lors de l'échange de documents. Dans l'attente d'un support complet des deux normes dans les suites les plus utilisées, des méthodes de transformation sont disponibles (ex : [ODF Converter](#), [Plugin ODF](#) de Sun).

Cette fiche est fondée sur les informations disponibles au mois de mai 2009 et sera révisée d'ici la publication officielle du référentiel si de nouveaux éléments d'appréciation se faisaient jour.

3.2.2. Echange de documents bureautiques non révisables

La plupart des documents bureautiques échangés ont un but informatif et ne sont pas destinés à être révisés. Il est réellement bénéfique d'échanger des documents dans un format ouvert et parfaitement interopérable.

Le format PDF 1.7 a été normalisé par l'ISO en juillet 2008 et ses spécifications rendues publiques. Avant cette normalisation, le format PDF était devenu un standard de fait de par son adoption par la très grande majorité des utilisateurs.

Un des principaux avantages de ce format réside dans le fait que les documents transformés au format PDF sont parfaitement fidèles aux documents originaux. Les polices, les images, les objets graphiques et la mise en forme du fichier source sont préservés, quelles que soient l'application et la plate-forme utilisées pour créer ces documents.

Recommandé	PDF	ISO	
Il est RECOMMANDÉ d'utiliser le format PDF 1.7, pour les échanges de documents bureautiques en mode non révisable.			

3.2.3. Archivage de documents bureautiques non révisables statiques

Le format PDF/A-1 décrit dans la norme ISO 19005-1, répond aux problématiques d'archivage à long terme. Toutes les informations nécessaires à la représentation du document sont incluses dans le fichier, telles que les polices de caractères, les images et les informations colorimétriques. Si le PDF 1.7 (plus léger) est adapté aux échanges, le PDF/A est, quant à lui, utilisé dans le cadre de la conservation et de l'archivage.

Il est important de noter qu'il y a deux variantes de PDF/A-1.

- La version PDF/A-1a représente la forme complète de la norme ISO ;
- La version PDF/A-1b représente une forme allégée de la norme ISO. Cette version préserve la lisibilité du document et sa bonne présentation à l'affichage et à l'impression.

Recommandé	PDF/A	ISO	
Il est RECOMMANDÉ d'utiliser le format PDF/A, pour l'archivage des documents bureautiques statiques non révisables.			

Remarque : dans le cas d'échange de documents archivés dans le format PDF/A, il n'est pas nécessaire de les convertir au format PDF 1.7 avant échange.

3.2.4. Conservation des documents bureautiques dynamiques

Le format PDF/A-1 est basé sur le format PDF v1.4. Il s'agit donc d'une version restreinte du format PDF.

Les restrictions sont caractérisées par :

- La non inclusion d'objets dynamiques de type audio ou vidéo,
- L'interdiction du lancement de code script ou de fichiers exécutables,
- L'interdiction du chiffrement et de la sécurité.

Du fait de la limitation actuelle des fonctionnalités du PDF/A, il est conseillé d'utiliser le PDF 1.7, qui prend en compte les aspects dynamiques des documents. Cependant, il faut noter que ce format n'est pas dédié à l'archivage, contrairement à PDF/A.

Recommandé	PDF 1.7	ISO	
Il est RECOMMANDÉ d'utiliser le format PDF 1.7 pour la conservation des documents bureautiques dynamiques.			

Des évolutions de la norme PDF/A sont en cours, ces travaux sont basés sur le format PDF 1.6 et prennent en compte les aspects dynamiques d'un document bureautique.

3.2.5. Echange de données numériques d'impression

Le format PDF/X a été défini en 1998 par le groupe de travail CGATS (*Committee for Graphic Arts Technology Standards*), sur l'initiative du DDAP (*Digital Distribution of Advertising for Publications*) et du NAA (*Newspaper Association of America*). Ce format de fichier est adapté aux problématiques d'impression. La spécification proposée par le groupe de travail CGATS a été adoptée plus tard par l'ISO.

Les spécifications de ce format permettent d'assurer l'échange de documents PDF de manière fiable dans le domaine de la pré-impression. Les fichiers PDF sont vérifiés avant leur envoi de façon à éviter les différences d'interprétation des RIP Postscript. La lettre "/X" signifie Blind eXchange (échange aveugle). L'objectif de PDF/X est de permettre un "échange aveugle" de fichiers PDF dans un flux de production graphique.

La norme ISO 15930 se décline, à ce jour, en plusieurs versions :

- PDF/X-1a (ISO 15930-1) : cette version est basée sur la version PDF 1.3. Elle est utilisée dans des environnements adaptés et présente la particularité de pouvoir incorporer les images haute résolution en fichiers attachés. Cette version est utilisée pour l'échange complet de données numériques ;
- PDF/X-2 (ISO 15930-2) : cette version n'oblige pas l'incorporation des polices et des images haute résolution. Elle permet donc l'échange de documents avec des ressources partielles, car c'est à la réception que les ressources nécessaires seront complétées. Elle n'oblige pas l'incorporation des images haute résolution ni des polices et ne peut donc être utilisée dans un environnement ouvert. Cette version ne peut être utilisée pour une impression professionnelle ;
- PDF/X-3 (ISO 15930-3 et 15930-6) : cette version est basée sur les versions PDF 1.3 et PDF 1.4. Elle autorise les gestions de la couleur plus étendue que le PDF/X-1a. Elle oblige l'encapsulation des polices utilisées et n'interdit pas les compressions du document, mais ne nécessite pas de connaître l'environnement dans lequel ont été préparés les fichiers PDF (principe de l'échange aveugle). Elle représente à ce jour le meilleur compromis entre liberté de création, fiabilité et possibilités de corrections ;
- PDF/X-4 (ISO 15930-7) : cette version concerne l'échange complet de données d'impression (PDF/X-4) et l'échange partiel de données d'impression avec une référence de profil externe (PDF/X-4p) par utilisation du format PDF 1.6. Elle a été publiée en février 2008.

La version PDF/X-5 est encore en cours d'élaboration au sein de l'ISO. Elle repose sur l'utilisation de la version PDF 1.6.

Recommandé	PDF/X	ISO	
Il est RECOMMANDÉ d'utiliser le format PDF/X pour l'échange de données numériques d'impression.			

3.2.6. Echange de documents structurés

Un document structuré est un document supportant un format dont chaque élément est parfaitement défini.

XML (*Extensible Markup Language*) est un langage basé sur le langage SGML (ISO 8879). Il a été défini et promu par le consortium W3C.

XML 1.1 a été conçu pour assurer une prise en charge plus étendue des caractères Unicode.

Le W3C recommande aux processeurs XML de reconnaître les deux versions.

Recommandé	XML	W3C	
Il est RECOMMANDÉ d'utiliser le langage XML pour l'envoi de documents structurés.			

 XML peut également être utilisé dans le cadre de l'exportation de base de données. Se reporter au chapitre 3.1.9 *Exportation de bases de données*

3.2.7. Langage de transformation de données structurées

Le langage XSLT (*eXtensible Stylesheet Language Transformations*), spécifié par le W3C, permet de transformer des documents XML en documents XML ou en documents s'appuyant sur d'autres formats. XSLT est souvent utilisé pour transformer le schéma de document XML ou pour convertir du XML en HTML ou XHTML.

Pour accéder aux données XML, le développeur dispose d'expressions formalisées en langage XPath spécifié également par le W3C. XPath est un langage de requête qui permet de naviguer à travers l'arborescence d'un document XML et de sélectionner des nœuds spécifiques selon une large variété de critères.

Recommandé	XSLT / XPath	W3C	 
Il est RECOMMANDÉ d'utiliser les langages XSLT et XPath pour formater et transformer des documents XML.			

3.2.8. Service de compression de fichiers

La compression de données est une technique qui permet de réduire l'espace nécessaire à la représentation d'une certaine quantité d'information. Elle concerne ainsi la transmission des données en ligne mais également leur sauvegarde dans un fichier. Cette fiche traite exclusivement du thème de la compression des fichiers de données.

Zip est un format créé en 1989 par la société PKWARE. S'il s'agit d'un format propriétaire, ses spécifications sont publiques depuis sa création et l'implémentation d'une grande partie de ses fonctions se fait sous licence ouverte (il utilise en particulier l'algorithme « deflate » défini dans le RFC 1951).

Zip est le format de compression de fichiers le plus répandu à travers le monde, il est implémenté dans une multitude d'outils et supporté nativement dans les dernières versions de Windows et Mac OS.

Certaines méthodes de compression telles que 7z, Rar ou Rk proposent des taux de compression plus performants mais impliquent l'installation de clients. De plus, le nombre de logiciels de compression proposant leurs implémentations est limité.

Recommandé	Zip	PKWARE	
Il est RECOMMANDÉ d'utiliser le format Zip pour la compression de fichier dans un but d'échange.			

 Sur cette même problématique de compression, voir le chapitre *4.4.2.5 Meilleures pratiques HTTP*

3.2.9. Syndication de contenu

RSS (*Really Simple Syndication*) décrit un format de document XML permettant de réaliser de l'agrégation (de la syndication) de contenu Web. C'est un langage simple de formatage des données. Ce format est habituellement utilisé pour obtenir les mises à jour d'informations dont la nature change fréquemment. Pour recevoir ces mises à jour, l'utilisateur s'abonne à un flux (ou fil) d'information.

RSS peut être utilisé de deux manières :

- Agrégation au niveau d'un portail des contenus provenant de différents services,
- Accès à des contenus directement du poste de travail de l'utilisateur à l'aide d'un lecteur de flux RSS.

Le format de syndication ATOM a été créé pour combler certaines lacunes de RSS. Il se distingue notamment sur les éléments suivants :

- Identification du type de flux transporté,
- Alignement avec les formats de date ISO,
- Gestion du multilinguisme.

Ce format est standardisé et maintenu par l'IETF.

Recommandé	RSS / ATOM	RSS Board / IETF	
Il est RECOMMANDÉ d'utiliser les formats RSS et/ou ATOM pour réaliser de la syndication de contenu Web de type « fil d'information ».			

Pour une mise en œuvre des techniques de syndication de contenu favorisant l'interopérabilité, il est utile de préciser aux navigateurs le type de contenu (ou type MIME - Internet Media Type) des fils d'informations envoyés.

Recommandé	Type de contenu des fils d'information
Afin de préciser le type de contenu des fils d'informations envoyés aux navigateurs, il est RECOMMANDÉ de positionner le paramètre HTTP Content-Type header aux valeurs « text/xml », « application/rss+xml » ou « application/atom+xml ».	

4. Interopérabilité technique

Le RGI regroupe les normes et standards techniques selon quatre grands domaines :

- La présentation
La présentation traite des technologies de navigation et de restitution.
- Le multimédia
Le multimédia traite des technologies de communication entre humains, notamment de la messagerie et de la téléphonie.
- Les services web
Les services web traitent des technologies d'échanges entre SI.
- L'infrastructure
L'infrastructure traite des technologies élémentaires nécessaires aux échanges, notamment des protocoles réseau.

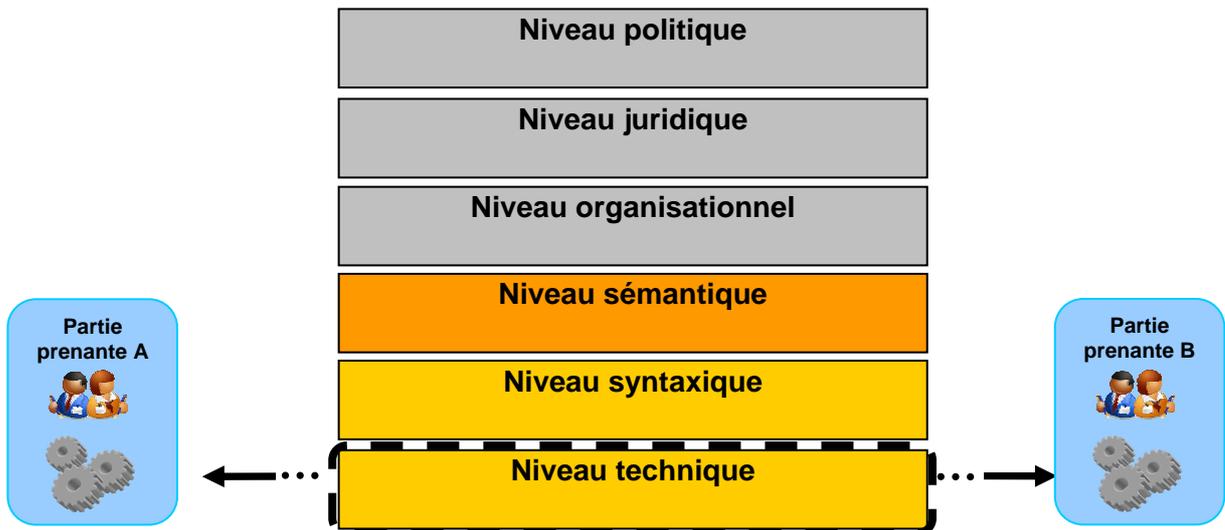


Figure 17 : Le niveau technique

4.1. Présentation

4.1.1. Technologies pour construire les IHM

Le langage HTML (*Hypertext Markup Language*) est un langage créé et utilisé pour écrire des pages Web. Il est conforme à la norme ISO 8879 qui décrit le langage SGML (*Standard Generalized Markup Language*). Il permet notamment d'insérer des liens dans du texte, ce qui autorise une navigation de page en page. Depuis 1999 le langage XHTML (*Extensible HyperText Markup Language*) a succédé au langage HTML. Sa principale force réside dans le fait qu'il dissocie la forme d'une page web de son contenu.

Le langage XHTML respecte la syntaxe définie par le langage XML.

Recommandé	XHTML	W3C	
Il est RECOMMANDÉ d'utiliser le langage XHTML pour construire les interfaces des sites Internet de l'administration.			

Il existe trois types de syntaxe du langage XHTML :

- XHTML 1.0 Strict : cette grammaire est la plus stricte et interdit l'utilisation des attributs dépréciés d'HTML,
- XHTML 1.0 Transitionnel : cette grammaire permet l'utilisation de certains attributs de présentation dépréciés,
- XHTML 1.0 Frameset : cette grammaire autorise l'utilisation de frames

Recommandé	XHTML strict	W3C	
Il est RECOMMANDÉ d'utiliser la syntaxe « XHTML 1.0 Strict » ou « XHTML 1.0 Transitionnel » pour construire les interfaces des sites Internet de l'administration.			

En observation	HTML 5	W3C	
Un groupe de travail, soutenu par les principaux éditeurs de navigateurs Internet, a été créé par le W3C pour faire à nouveau évoluer le langage HTML. Les premières versions de travail des spécifications HTML 5 ont été publiées.			

4.1.2. Feuilles de styles

Les feuilles de style en cascade CSS (*Cascading Style Sheet*) permettent de spécifier l'habillage et la mise en page (couleurs, polices, rendu) des documents structurés (XHTML, XML, etc.) mais aussi des IHM des applications Web de l'administration électronique. Le niveau 2 de CSS permet notamment d'adapter la présentation à différents modes d'accès de l'utilisateur (navigateurs graphiques, imprimantes, terminaux braille, etc.).

Recommandé	CSS 2	W3C	
Il est RECOMMANDÉ d'utiliser les feuilles de style CSS niveau 2 pour ajuster la présentation de documents structurés.			

En observation	CSS 3	W3C	
Le W3C travaille actuellement sur la version 3 de CSS, qui sépare en modules distincts les différentes fonctionnalités des feuilles de styles.			

4.1.3. Utilisation de scripts

En informatique, le langage de script est utilisé pour mettre au point rapidement des programmes. Il s'agit en effet d'une suite d'instructions interprétées et exécutées dans l'ordre où elles sont écrites.

Dans le contexte des applications du Web, le script est intégré à une page Web et exécuté par le navigateur. Il permet de réaliser des tâches simples comme la vérification des données entrées dans un formulaire, la gestion des menus, etc.

Javascript est une implémentation largement usitée de la norme ISO ECMAScript. La majorité des navigateurs web du marché l'implémentent.



La notation JSON permet le traitement des données échangées directement dans Javascript.

Il faut noter l'existence de frameworks de scripts, qui sont des bibliothèques regroupant un certain nombre de fonctions et méthodes Javascript. Ces bibliothèques permettent de faciliter le développement et d'assurer une portabilité optimale.

Lors de l'utilisation de scripts, il est important de prévoir un accès dégradé à l'information pour les usagers ayant désactivé les fonctions de scripts.

Recommandé	ECMAScript	ISO	
Pour l'utilisation de scripts, il est RECOMMANDÉ d'utiliser des langages conformes à la norme de langage ECMAScript ; dans le cas d'utilisation de frameworks, le choix doit se porter sur des frameworks pérennes et supportés par une communauté importante.			

4.1.4. Navigateurs web

Depuis quelques années, il y a une diversification des types d'appareils permettant d'accéder au Web. Chaque type d'appareil possède sa propre IHM (Interface Homme Machine). Cette diversification est principalement due au développement des possibilités de mobilité.

Les développeurs auront le souci de rendre les développements logiciels indépendants de leur support matériel et de s'assurer de la compatibilité des services en ligne avec les principaux navigateurs du marché.

Recommandé	Navigateurs
Il est RECOMMANDÉ de s'assurer de la compatibilité des services en ligne avec les navigateurs Web suivants :	
<ul style="list-style-type: none">• Internet Explorer (version 6 et supérieures),• Mozilla Firefox (version 2 et supérieures),• Safari (version 3 et supérieures).	

 Afin de favoriser l'accessibilité, il est conseillé de s'assurer de la lisibilité des services en ligne dans des navigateurs de type texte comme [Lynx](#). Pour plus d'information sur l'accessibilité, se reporter au [RGAA](#).

Lors de la conception / réalisation d'un site internet, il est possible



- de vérifier [la syntaxe des documents web](#),
- de valider [la syntaxe des feuilles de style](#),
- d'évaluer l'ergonomie du site au regard de la « [Charte Ergonomique](#) ».

4.2. Multimédia

4.2.1. Messagerie

4.2.1.1. Protocole de messagerie

SMTP (*Simple Mail Transfer Protocol*) est le protocole utilisé pour le transport des messages électroniques (appelés aussi courriers électroniques ou courriels) sur Internet.

Le protocole SMTP permet le transfert du courrier électronique selon un procédé efficace et fiable. Il est basé sur la couche transport TCP et donc conforme au protocole IP.

Les principes de base sont référencés par les recommandations RFC 2821 pour la spécification de base et RFC 2822 pour le format des messages.

Règle 01	SMTP	IETF	
Pour l'échange de courriels, il est OBLIGATOIRE d'utiliser le protocole SMTP.			

Notons aussi que la recommandation RFC 2821 prévoit l'utilisation d'extensions SMTP (ESMTP) en fournissant une structure pour la prise en charge de fonctionnalités additionnelles.

Recommandé	ESMTP	IETF	
Il est RECOMMANDÉ d'utiliser l'extension ESMTP pour implémenter les fonctionnalités supplémentaires au protocole SMTP.			

4.2.1.2. Représentation des messages et des pièces jointes

Les spécifications de SMTP ne couvrent pas l'ensemble des formats tels que les images, les fichiers binaires ou les messages imbriqués. De plus, elles ne supportent que les jeux de caractères ASCII.

MIME (*Multipurpose Internet Mail Extensions*) est un format d'échange de message utilisé pour la représentation des messages électroniques. Il comble les lacunes de SMTP en définissant comment coder les textes non ASCII et les pièces jointes, de sorte qu'ils puissent être véhiculés au sein du RFC 2822.

Son usage est obligatoire pour l'envoi de courriels aux usagers et aux agents publics.

Règle 02	MIME	IETF	
Pour la représentation des courriels et des pièces jointes, il est OBLIGATOIRE d'utiliser le format d'échange MIME.			

4.2.1.3. Sécurisation de la messagerie

S/MIME est une extension de MIME qui permet de sécuriser des messages MIME (chiffrement ou signature). Son usage est obligatoire pour l'envoi sécurisé de courriels aux usagers et aux agents publics.

Règle 03	S/MIME	IETF	
Pour sécuriser les envois de courriels, il est OBLIGATOIRE d'utiliser l'extension S/MIME.			

STARTTLS est une extension du protocole SMTP permettant de sécuriser une transaction en créant un tunnel TLS entre deux serveurs de messagerie.

Recommandé	STARTTLS	IETF	
Il est RECOMMANDÉ de proposer l'extension ESMTP STARTTLS sur les serveurs de messagerie, mais sans exiger que les clients l'utilisent (en particulier entre serveurs ou sur Internet).			

4.2.1.4. Accès aux boîtes aux lettres électroniques

POP3 et IMAP4 sont des protocoles utilisés pour l'accès aux BAL (Boîtes Aux Lettres électroniques).

IMAP (*Interactive Mail Access Protocol*) est moins utilisé que POP3 mais il offre plus de possibilités. Il gère plusieurs accès simultanés, ainsi que plusieurs boîtes aux lettres sur le serveur. Il permet aussi les recherches de courrier selon des critères. Il est plus riche mais plus complexe à mettre en œuvre que POP3.

IMAP4 devrait progressivement remplacer POP3.

Règle 04	POP3 / IMAP4	IETF	
Pour relever les courriels déposés dans une boîte aux lettres, il est OBLIGATOIRE de pouvoir mettre en œuvre le protocole POP3 ou le protocole IMAP4.			

4.2.1.5. Les services de messagerie instantanée

La messagerie instantanée est un service qui permet de communiquer par ordinateur avec un interlocuteur distant connecté au même réseau informatique, notamment Internet. On parle de dialogue en ligne (« chat » en anglais).

En évoluant, la messagerie instantanée tend à intégrer des fonctionnalités de voix sur IP ainsi que de visioconférence grâce à l'adjonction d'une caméra et d'un microphone. Elle s'ouvre également à la communication entre processus automatisés et/ou ordinateur et serveurs.

Face à l'absence d'interopérabilité entre les protocoles propriétaires existants, l'IETF a proposé en 2004 le protocole XMPP pour pouvoir opérer des services de messagerie instantanée sur Internet, de manière ouverte et non propriétaire.

XMPP est l'acronyme de « *eXtensible Messaging and Presence Protocol* » que l'on peut traduire en français par « protocole extensible de présence et de messagerie ». Il est basé sur une architecture client/serveur permettant les échanges décentralisés de messages instantanés ou non entre les clients. Il est défini par les RFC 3920 à 3923.

Le protocole XMPP réalise ses échanges de données par transmission de flux XML. Cela lui offre des possibilités d'extension très importantes et il peut ainsi être utilisé dans des applications et environnements très divers.

XMPP présente une architecture de type client/serveur (C2S) et serveur à serveur (S2S). Les communications se font donc entre les clients et le serveur et entre les serveurs, comme l'e-mail, à ceci près qu'un serveur XMPP est à la fois émetteur et récepteur de messages instantanés et de présence.

Un environnement XMPP repose sur deux grands groupes de spécifications :

- Le premier est le socle de base que constituent les RFC de l'IETF consacrées au cœur du protocole XMPP. Ce socle est obligatoire pour que l'infrastructure fonctionne ;
- Le second est constitué par les XEP (*XMPP Extension Protocol*) qui regroupent un ensemble d'extensions pour ajouter de nouvelles fonctionnalités. Ces extensions sont facultatives aussi bien pour les clients que pour les serveurs.

Recommandé	XMPP	IETF	
Il est RECOMMANDÉ d'utiliser XMPP pour la messagerie instantanée.			



Concernant la sécurisation des communications échangées, XMPP utilise le protocole TLS. Ce protocole est détaillé au chapitre 4.4.2.8 *Service de sécurisation des échanges*

4.2.2. Téléphonie

4.2.2.1. Protocoles pour la téléphonie

La voix sur réseau IP souvent abrégée en « VoIP » (*Voice over IP*), est une technique qui permet de transporter des conversations téléphoniques sur tout réseau acceptant le protocole IP. La technique utilisée est une encapsulation des données dans les paquets IP. C'est une technique très différente de la téléphonie classique qui dépend de centraux téléphoniques (autocommutateurs) et d'un câblage dédié.

La téléphonie sur réseau IP souvent abrégée en « ToIP » (*Telephony over IP*), est une technique qui permet de transporter des conversations téléphoniques sur tout réseau acceptant le protocole IP, mais également de fournir des services comparables à ceux délivrés par un autocommutateur téléphonique classique.

Les protocoles RTP et RTCP sont de niveau Transport (modèle OSI couche 4) mais sont placés au-dessus du protocole de transport UDP. Le protocole UDP est léger donc rapide et a l'avantage d'être multi-cast. Le protocole TCP est trop lent pour envisager de faire du temps réel sur IP.

RTP est spécifié par l'IETF et s'appuie sur un ancien protocole propriétaire, RDP.

Le protocole RTCP (*Real-time Transfert Control Protocol*) est un protocole associé à RTP. Il est basé sur des transmissions périodiques de paquets de contrôle par tous les participants dans la session. Il contrôle les flux RTP et permet de véhiculer des informations basiques sur les participants d'une session et sur la qualité de service. Néanmoins si RTCP mesure les performances, il n'offre pas de garantie de service.

Recommandé	RTP / RTCP	IETF	
Il est RECOMMANDÉ d'utiliser le protocole RTP et son protocole de contrôle de flux RTCP pour le transport de la voix sur protocole IP.			

Sécurité des médias : pour information, la protection des médias (données, vidéo, voix) est un point sensible des architectures de téléphonie. Le protocole RTP/RTCP permet de gérer les flux de données au niveau média mais ils ne sont pas sécurisés. Le protocole SRTP/SRTCP peut permettre de sécuriser les flux médias.

 RTP peut également être utilisé dans le cadre de la 4.4.2.9 *Diffusion vidéo en mode continu*

4.2.2.2. Signalisation et gestion de session

4.2.2.2.1. Le protocole H.323

Le protocole H.323 regroupe un ensemble de protocoles de communication sur le protocole IP. H.323 assure des services pour communications multimédia sur des réseaux en mode paquet n'offrant pas nécessairement une qualité de service garantie. Les entités H.323 peuvent assurer en temps réel des communications audio, vidéo et de données. Seul le mode audio est obligatoire.

Le réseau à commutation de paquets sur lequel communiquent les entités H.323 peut être constitué d'une connexion point à point, d'un seul segment ou d'un inter-réseau de plusieurs segments aux topologies complexes. C'est un protocole développé par l'UIT-T. Il est dérivé du protocole H.320 utilisé sur les réseaux RNIS.

Terminal : un terminal H.323 est une extrémité du réseau assurant en temps réel des communications bidirectionnelles avec un autre terminal, une autre passerelle ou un autre pont de conférence H.323. Ces communications permettent l'échange de commandes, d'indications, de signaux audio, d'images animées vidéo en couleur et/ou de données entre les deux terminaux.

Signalisation : H.323 décrit l'utilisation de trois types différents de messages: H.245, RAS et signalisation d'appel H.225.0.

Le module de commande du système (H.245, H.225.0) assure la signalisation nécessaire au bon fonctionnement du terminal H.323. Il assure la commande d'appel, l'échange des capacités, la signalisation des commandes et des indications et il fournit des messages d'ouverture des voies logiques.

RTP/RTCP : Dans certains cas, l'utilisation du protocole RTP/RTCP est requise par exemple pour les chiffres DTMF (*Dual Tone Multi Frequency*), les tonalités et les signaux téléphoniques.

Chiffrement : Les fonctions d'authentification et de sécurité sont facultatives pour les systèmes H.323. Si toutefois elles sont fournies, elles doivent l'être conformément à la Rec. UIT-T H.235.0

Applications de passerelle : Il existe de nombreuses applications pour passerelles décomposées et composites. Les vendeurs et/ou les exploitants peuvent décider d'utiliser une passerelle composite ou décomposée selon les exigences applicatives. Les passerelles décomposées sont appelées par la Rec. UIT-T H.248 à interfonctionner avec les passerelles composites.

Recommandé	H.323	UIT	
Il est RECOMMANDÉ d'utiliser le protocole H.323 pour l'établissement de sessions de communication multimédia lorsque le transport sous-jacent est un réseau en mode paquet.			

4.2.2.2. Protocole d'initialisation de session

Le protocole d'initialisation de session ou SIP (*Session Initiation Protocol*) travaille de concert avec des protocoles permettant aux points de terminaison Internet (appelés agents utilisateurs) de se découvrir l'un l'autre et de se mettre d'accord sur une caractérisation d'une session qu'ils aimeraient partager. Pour localiser les participants potentiels à une session et pour d'autres fonctions, SIP permet la création d'une infrastructure d'hôtes de réseau (appelés serveurs mandataires) auxquels les agents utilisateurs peuvent envoyer leurs enregistrements, invitations aux sessions et autres requêtes.

SIP est un outil souple et général pour créer, modifier et terminer les sessions multimédia. Il travaille indépendamment des protocoles de transport sous jacents et est indépendant du type de session établie.

SIP n'est pas un système de communications intégré verticalement mais un composant qui peut être utilisé avec d'autres protocoles de l'IETF pour construire une architecture multimédia complète.

Ces architectures incluent généralement des protocoles tels que :

- RTP (*Real-Time Transport Protocol*) : un protocole pour le transport en temps réel de données et la fourniture d'informations en retour sur la qualité de service,
- RTSP (*Real-Time Streaming Protocol*) : un protocole de communication permettant de contrôler un serveur de média à distance,
- MEGACO/H248 (*Media Gateway Control Protocol*) : un protocole pour contrôler des passerelles vers le réseau téléphonique public commuté (RTPC),
- SDP (*Session Description Protocol*) : un protocole de description de session multimédia.

SIP devrait être utilisé conjointement avec les autres protocoles afin de fournir des services complets aux utilisateurs. Cependant, le fonctionnement de base de SIP ne dépend d'aucun de ces protocoles.

Recommandé	SIP	IETF	
Il est RECOMMANDÉ d'utiliser SIP, pour établir, modifier et terminer des sessions multimédia (conférences) telles que des communications téléphoniques par l'Internet.			

 La protection du protocole SIP est un point sensible des architectures de téléphonie. Le protocole TLS peut permettre de sécuriser les flux de signalisation. Ce protocole est détaillé au chapitre 4.4.2.8 *Service de sécurisation des échanges*

4.2.2.3. Codage de voix

Il existe de nombreuses manières de coder la voix. Les travaux l'UIT-T et de l'ETSI font référence en la matière.

Pour une transmission de la voix, sans compression, la bande passante est de 64 kbps en utilisant un codage tel que le codec G.711. Le codec G.711 est utilisé en téléphonie classique RTC ou RNIS et en VoIP.

Il existe d'autres spécifications de codage/décodage (codecs):

- La famille de codecs G.729 est utilisée pour le codage de la parole 8kbits/s pour obtenir une téléphonie de qualité, la visio-conférence et la VoIP ;
- Le codec G.723.1 est utilisé en VoIP et plus particulièrement pour les communications multimédias acheminées à 5,3 kbit/s et à 6,3 kbit/s ;
- Le codec G.726 est utilisé en téléphonie satellite et en VoIP, pour la modulation par impulsions et le codage différentiel adaptatif (MICDA) à 40, 32, 24, 16 kbit/s ;
- Le codec G.722 est utilisé pour le codage audiofréquence à 7 kHz à un débit inférieur ou égal à 64 kbit/s.

Il est important de préciser que le débit mentionné est relatif à la couche applicative. Le débit réel engendré au niveau IP ou Ethernet est nécessairement plus important du fait de l'encapsulation.

Recommandé	Codecs téléphonie	ETSI, UIT-T, GSM, 3PPP
Il est RECOMMANDÉ d'utiliser un ou plusieurs codecs parmi ceux spécifiés dans les recommandations G.711A , G.722 , G723.1 , G.729 , G.729A , ETSI GSM 06.10 , IETF iLBC , Speex , pour le codage de la voix.		

Attention : le choix d'un ou plusieurs codecs se fera en fonction des caractéristiques du réseau utilisé.

Dans la pratique, l'ensemble des codecs indiqués ci-dessus n'est pas implémenté dans chaque poste IP. A l'heure actuelle, les postes IP supportent G729, G711 et parfois G722. Le support des codecs GSM 06.10, iLBC et Speex est de fait assez rare.

Liste des codecs audio du GSM et de l'UMTS

Les standards du GERAN et de l'UTRAN proposent 40 différents codecs de voix (3GPP TS 26.103 V8.1.0) :

- pour le GSM avant la Rel-4 : GERAN séries 06,
- pour le GSM Rel-4 et suivantes : GERAN séries 46,
- pour la 3G/GSM (R99 et autres) : GERAN + UTRAN séries 26.

4.2.2.4. Annulation d'écho

Que ce soit sur des réseaux analogiques ou sur des réseaux numériques, il est nécessaire de mettre en œuvre des dispositifs d'annulation d'écho ou de suppression d'écho. L'UIT en a spécifié plusieurs ; certains sont compatibles entre eux, comme par exemple G.164 et G.165.

L'écho a un effet majeur sur la qualité de la voix dans les réseaux de télécommunication. Les effets indésirables de l'écho résultent des combinaisons de réflexions venant des composants du réseau, combinées avec le signal et le délai de transmission. L'écho peut causer des difficultés de parole et d'écoute pour l'utilisateur de la connexion téléphonique. Il peut aussi perturber les transmissions des données de la bande voix, fax et télétexe.

Les annulations d'échos du réseau numérique sont faites pour éliminer l'écho pour l'utilisateur et pour faciliter les transmissions des données de la bande voix et fax.

Une bonne pratique consiste à utiliser la recommandation G.168 (UIT-T G.168) comme dispositif d'annulation d'écho sur les réseaux numériques.

Bien que l'annulation d'écho ne nécessite pas d'interaction entre les équipements, il est bon de préciser ce point pour garantir l'interopérabilité des solutions de téléphonie. Cela permet d'éviter des interactions néfastes entre annulations d'écho incompatibles.

Recommandé	G.168	UIT-T	
Il est RECOMMANDÉ d'utiliser la recommandation G.168 comme dispositif d'annulation d'écho sur les réseaux numériques.			

4.2.2.5. Convergence des messageries

Les utilisateurs sont confrontés à une multiplication des systèmes de messagerie tels que la messagerie de l'ordinateur, la boîte vocale du téléphone fixe et celle du téléphone portable, les messageries des ordinateurs de poche et les SMS (*Short Message Service*) sur téléphone portable.

La convergence des messageries devient une nécessité.

Un exemple de convergence consiste à transformer les messages vocaux en fichiers. Ces fichiers sont transmis sur la messagerie de l'ordinateur comme pièce jointe d'un message classique. Dans le cadre d'une messagerie unifiée, le format MP3 permet d'archiver des messages audio en provenance d'une messagerie vocale. La taille des messages au format MP3 est plus petite que celle des messages utilisant des formats non compressés.

Dans le serveur vocal, les messages nécessitent ainsi moins d'espace de stockage que des messages utilisant des formats non compressés.

Recommandé	MP3	ISO	
Il est RECOMMANDÉ d'utiliser le format MP3 pour enregistrer les messages vocaux mis en pièce jointe dans les messageries unifiées.			

En observation	Vorbis	Xiph	
De conception moderne, le codec Vorbis, qui est un format ouvert, offre une meilleure qualité et un meilleur taux de compression que le format MP3. Cependant, malgré une adoption croissante, il est aujourd'hui moins implémenté que le format MP3.			

En observation	Speex	Xiph	
Speex est codec spécialisé dans les applications de VoIP/ToIP de plus en plus utilisé. Etant dédié à la voix humaine, il propose un excellent taux de compression dans ce domaine, tout en conservant une très bonne qualité.			

 Concernant les formats audio, se reporter au chapitre 3.1.4 *Formats de séquence sonore*

4.3. Services Web

Ce chapitre présente les normes, standards et meilleures pratiques à mettre en œuvre afin de garantir l'interopérabilité des Services Web, c'est à dire permettre à une autorité administrative de consommer des services mis à disposition par d'autres administrations et d'exposer ses propres services à des clients (administrations, usagers, ...).

Les Services Web sont des composants informatiques exposant des fonctions sur le réseau (Internet, intranet). Ils doivent supporter des interactions et des échanges de données normalisées dans un environnement distribué, de manière indépendante des technologies d'implémentation utilisées.

L'acception Services Web englobe les deux technologies suivantes :

- Les Services Web SOAP (*Simple Object Access Protocol*),
- Les Services Web REST (*Representational State Transfer*).

Par ailleurs, l'administration a défini PRESTO, un protocole d'échanges de messages informatiques entre applications basé sur les Services Web SOAP.

Pour les échanges fréquents de petites volumétries en mode requête-réponse, les services Web REST et SOAP sont les plus utilisés.

Pour les échanges nécessitant accusé de réception, fiabilité, intégrité et confidentialité, le protocole PRESTO est approprié.

Pour les échanges de fichiers ne nécessitant ni d'accusé de réception, ni de mise en place de mécanismes de reprise, il est possible d'utiliser S-FTP (voir le chapitre consacré aux *Services de transfert de fichiers*).

4.3.1. Protocole d'échange des messages de l'administration

Les échanges entre les SI des administrations sont de plus en plus nombreux et concernent toutes les autorités administratives (administrations centrales, organismes de protection sociale, collectivités territoriales, etc.). Les solutions permettant ces échanges électroniques sont nombreuses : développement interne, utilisation de progiciels, choix d'un tiers de télétransmission, etc.

Dans le cadre d'une démarche d'informatisation et d'urbanisation des échanges électroniques, PRESTO (PRotocol d'Echanges STandard Ouvert de l'Administration), un protocole d'échange de données, a été développé afin de répondre à la majorité des besoins et avec le but de véhiculer les messages informatiques entre les applications des SI des autorités administratives.

Ce profil repose sur des spécifications de profils du WS-I (Basic Profile et Security Profile) et sur des spécifications du W3C et de l'OASIS.

Recommandé	PRESTO	DGME	
Il est RECOMMANDÉ d'utiliser le protocole PRESTO v1.1 pour les échanges de messages entre administrations.			

4.3.2. Les Services Web SOAP

4.3.2.1. Protocole de services

SOAP (*Simple Object Access Protocol*) est un protocole qui fait l'objet d'une recommandation du W3C.

Il permet de définir des mécanismes d'échanges d'information structurée et a pour objectif d'assurer un dialogue entre composants distribués et décentralisés en utilisant la notation XML.

Si le transport des données est réalisé le plus souvent à l'aide du protocole HTTP, SOAP reste indépendant du protocole de transport (ex : SMTP peut être utilisé).

SOAP définit un format pour l'envoi des messages XML. Les messages SOAP sont structurés en un document XML qui comporte les éléments suivants :

- Une enveloppe obligatoire qui définit le contenu du message et contient :
 - Un en-tête optionnel qui inclut différentes informations (autorisations et transactions par exemple),
 - Un corps contenant les informations sur l'appel et la réponse.
- Des attachements optionnels.

Recommandé	SOAP	W3C	
Il est RECOMMANDÉ d'utiliser le protocole SOAP v1.1 ou SOAP v1.2 lors de la conception de Services Web SOAP.			

4.3.2.2. Langage de description de services

WSDL (*Web Services Description Language*) est un langage de description, qui fournit un modèle et un format XML pour décrire le contrat d'interface d'un Service Web. Il permet de séparer la description fonctionnelle abstraite d'un service, des détails concrets de son implémentation (tels que « comment » et « où » cette fonctionnalité est offerte).

Au niveau abstrait, WSDL décrit un Service Web en fonction des messages qu'il envoie et reçoit ; les messages sont décrits indépendamment d'un format de transmission particulier en utilisant un système de typage.

Au niveau concret, une liaison (*binding*) définit les détails des formats de transport et de transmission d'une ou plusieurs interfaces. Une extrémité (*port* ou *endpoint*) associe une adresse de réseau à une liaison. Enfin, un service regroupe les extrémités qui mettent en œuvre une interface commune.

Recommandé	WSDL v1.1	W3C	
Il est RECOMMANDÉ d'utiliser le langage WSDL v1.1 pour décrire les contrats d'interface des Services Web SOAP.			

4.3.2.3. Annuaire de services

UDDI (*Universal Description Discovery and Integration*) est une technologie d'annuaire basée sur le langage XML.

C'est une initiative ouverte de l'industrie, sponsorisée par l'OASIS, qui permet aux fournisseurs de publier la liste de leurs Services Web.

Un annuaire UDDI permet de localiser sur le réseau le Service Web recherché. Il repose sur le protocole de transport SOAP.

Recommandé	UDDI v2 / v3	OASIS	
Il est RECOMMANDÉ d'utiliser un annuaire UDDI v2 ou v3 pour la publication de Services Web SOAP.			

4.3.2.4. Profils d'utilisation

Le consortium WS-I (*The Web Service Interoperability Organization*) produit des recommandations pour les développeurs de Services Web afin de favoriser l'interopérabilité.

Le WS-I Basic Profile contient un ensemble de règles permettant de favoriser l'interopérabilité des Services Web SOAP.

Le Basic Profile v1.1 couvre les normes et spécifications suivantes :

- SOAP 1.1,
- RFC2616: Hypertext Transfer Protocol -- HTTP/1.1,
- RFC2965: HTTP State Management Mechanism,
- XML 1.0 (Second Edition),
- Namespaces in XML 1.0,
- XML Schema Part 1: Structures,
- XML Schema Part 2: Datatypes,
- WSDL 1.1,
- UDDI Version 2.04 API Specification, Dated 19 July 2002,
- UDDI Version 2.03 Data Structure Reference, Dated 19 July 2002,
- UDDI Version 2 XML Schema,
- RFC2818: HTTP Over TLS,
- RFC2246: The TLS Protocol Version 1.0,
- The SSL Protocol Version 3.0,
- RFC2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

Recommandé	Basic Profile v1.1	WS-I	
Il est RECOMMANDÉ de se conformer au profil d'utilisation « WS-I Basic Profile v1.1 ».			

Un fichier WSDL décrit le contrat d'interface d'un Service Web. Il peut être encodé de différentes façons :

- le style peut être soit 'RPC' soit 'document',
- l'encodage peut être soit 'literal' soit 'encoded'.

Pour harmoniser les pratiques et garantir l'interopérabilité, il est nécessaire de préférer l'encodage 'literal', conforme au profil WS-I.

Règle 05	Style d'échange et encodage	WS-I	
Pour les Services Web SOAP, il est OBLIGATOIRE d'utiliser le style d'échange « <i>document</i> » ou « <i>RPC</i> » et l'encodage « <i>literal</i> ».			

4.3.2.5. Pièces jointes

Pour associer à un message SOAP un objet binaire sous forme de pièce jointe, il est possible de suivre les recommandations du WS-I ou du W3C.

Le profil « Attachments v1.0 » du WS-I est composé d'un ensemble de spécifications ; elles complètent le Basic Profile v1.1 en normalisant le support des pièces jointes.

Le packaging XOP (*XML binary Optimized Packaging*) et le mécanisme MTOM (*Message Transmission Optimization Mechanism*) du W3C

- apportent une méthode standard pour associer des données binaires à un document XML au sein d'un paquet ;
- optimisent l'encodage et la transmission de messages SOAP.

Recommandé	Pièces jointes	WS-I / W3C	 
Pour des Services Web avec pièce jointe, il est RECOMMANDÉ de se conformer au profil d'utilisation « Attachments » du WS-I ou aux normes XOP/MTOM du W3C.			

4.3.2.6. Sécurisation

Le Basic Security Profile v1.0 est une extension du Basic Profile v1.0. Il est donc compatible avec celui-ci en lui ajoutant des spécifications de sécurité.

Le Basic Security Profile v1.0 est conçu pour supporter l'ajout de fonctionnalités de sécurité aux enveloppes et messages SOAP, ainsi qu'au niveau de la couche de transport des Services Web.

Recommandé	Basic Security Profile v1.0	WS-I	
Il est RECOMMANDÉ de se conformer au profil « Basic Security Profile v1.0 » pour sécuriser les services web SOAP.			

Le WSS (*Web Service Security*) est un standard de l'OASIS qui ajoute aux spécifications existantes une structure pour incorporer des mécanismes d'authentification, de signature et de chiffrement dans un message SOAP, utilisables lors de l'implémentation de Services Web.

Cette spécification est flexible et conçue pour sécuriser les Services Web avec une grande variété de modèles de sécurité, entre autres, l'utilisation de SAML, Kerberos et de certificats X.509.

Recommandé	WS-Security v1.1	OASIS	
Il est RECOMMANDÉ de se conformer au WS-Security v1.1 pour sécuriser les messages SOAP.			

4.3.3. Les Services Web REST

REST (*Representational State Transfer*) a été décrit par Roy Thomas Fielding dans sa thèse « *Architectural Styles and the Design of Network-based Software Architectures* ». C'est un style d'architecture et non un standard, il n'existe donc pas de spécifications de REST.

Dans une architecture REST, le composant de base est appelé ressource. Toute information qui peut être nommée est une ressource : un article de journal, une photo, un service ou n'importe quel concept. Une ressource est identifiée par un URI (*Uniform Resource Identifier*) qui permet de la nommer.

Pour invoquer des ressources, il faut utiliser les verbes HTTP :

- GET pour récupérer le contenu d'une ressource (recherche, lecture),
- POST pour créer une nouvelle ressource (mise à jour),
- PUT pour créer une ressource,
- DELETE pour supprimer une ressource.

Il faut noter que certains navigateurs n'implémentent pas les méthodes PUT et DELETE.

REST fait usage des standards éprouvés de l'architecture du Web :

- Utilisation du protocole HTTP, fournissant une interface uniforme pour accéder à toutes les ressources avec une interface générique (essentiellement les verbes GET, POST, PUT et DELETE),
- Utilisation des URI : chaque ressource du système est représentée (adressage et nommage) par une URI dont la connaissance doit suffire à accéder à la ressource,
- Utilisation de divers formats de la représentation des ressources : XML, (X)HTML, GIF, JPEG, Microformat, etc.
- Utilisation des types MIME pour la description de ces représentations : text/html, image/gif, image/jpeg, etc.

Atom est un format de document basé sur XML conçu pour la syndication de contenu périodique, tel que les sites d'actualités. Atom Publishing Protocol est un protocole informatique de création, modification et destruction de ressources Web.

Recommandé	Atom Publishing Protocol	IETF	
Il est RECOMMANDÉ d'utiliser le protocole Atom Publishing Protocol dans le cadre des Services Web REST.			

JSON (*JavaScript Object Notation*) est un format de données textuel, générique, dérivé de la notation des objets du langage ECMAScript. Il permet de représenter de l'information structurée.

Recommandé	JSON	IETF	
Il est RECOMMANDÉ d'utiliser le format de représentation JSON dans le cadre des Services Web REST.			

4.4. Infrastructure

4.4.1. Services d'annuaires et fédération d'identité

4.4.1.1. Annuaires LDAP

La question de l'interopérabilité des données entre annuaires consomme beaucoup de temps dans la gestion des SI. De nombreux annuaires coexistent au sein des entreprises et des entités administratives, comme l'annuaire téléphonique, l'annuaire d'intranet, l'annuaire de contrôleur de domaine réseau, l'annuaire dans les SI de gestion, etc. L'interopérabilité des données entre ces annuaires est problématique.

Originellement protocole d'interrogation et de modification de service d'annuaire, LDAP a évolué en tant que norme et définit dorénavant les fonctionnalités suivantes :

- un protocole réseau pour accéder à l'information contenue dans l'annuaire,
- un modèle d'information définissant la forme et le type de l'information contenue dans l'annuaire,
- un espace de nommage définissant comment l'information est organisée et référencée,
- un modèle fonctionnel définissant la manière d'accéder et de mettre à jour l'information,
- un modèle de distribution permettant de répartir les données (à partir de la version 3),
- un protocole et un modèle de données extensibles,
- des interfaces pour développer des applications clientes.

Règle 06	LDAP v3	IETF	
Il est OBLIGATOIRE de prévoir un mode d'accès conforme à LDAP v3 pour les annuaires interrogeables par plusieurs entités administratives.			

4.4.1.2. Echanges entre annuaires

LDIF (*LDAP Data Interchange Format*) permet de représenter les données LDAP sous un format texte harmonisé. Il est utilisé pour afficher ou modifier les données de la base. Il a vocation à donner une lisibilité des données à tout utilisateur. LDIF est également utilisé pour importer ou exporter des bases d'informations entre annuaires LDAP. La majorité des serveurs LDAP supportent ce format ce qui permet une grande interopérabilité entre eux.

Recommandé	LDIF	IETF	
Il est RECOMMANDÉ d'utiliser le format LDIF pour échanger tout ou partie d'un annuaire de données LDAP.			

Le langage DSML (*Directory Services Markup Language*) structure les données échangées entre annuaires. Ce langage constitue la principale ouverture des annuaires LDAP vers le monde XML. DSML peut être considéré comme l'ancêtre d'UDDI.

En observation	DSML	OASIS	
Le langage DSML (<i>Directory Services Markup Language</i>) est un langage basé sur XML. Il normalise les échanges de données entre des annuaires LDAP.			

4.4.1.3. Sécurisation des annuaires LDAP

Le protocole LDAP fournit des mécanismes de sécurité mis en œuvre pour garantir certains services de sécurité définis par l'ISO (ISO 7498-2) .

Le protocole TLS peut être utilisé avec LDAP afin de garantir l'intégrité et la confidentialité des échanges dans une communication entre applications LDAP et d'authentifier la connexion à un serveur LDAP.

Les éléments de sécurité pouvant être mis en œuvre par LDAPv3 sont les suivants :

- L'authentification des entités LDAP (serveurs, clients, données),
- La signature électronique des opérations effectuées sur l'annuaire,
- Le chiffrement de certaines données critiques de l'annuaire,
- Les règles d'accès (ACLs) aux données,
- L'audit du journal des opérations.

Enfin, LDAPv3 offre la possibilité d'accéder à un ensemble de fonctions de sécurité qui doivent être interopérables. C'est pourquoi un nombre minimum de ces fonctions doit être commun à toute implémentation supportant LDAPv3.

Recommandé	Extensions LDAP	IETF	
Pour sécuriser les services d'un annuaire de données LDAP, il est RECOMMANDÉ d'utiliser les extensions de sécurisation LDAP.			

 Pour plus de détails sur TLS, se reporter au chapitre 4.4.2.8 *Service de sécurisation des échanges*

4.4.1.4. Service de nom de domaine

Le service de nom de domaine DNS (*Domain Name System*) a pour vocation d'effectuer le lien entre une adresse Internet au format alphanumérique et son adresse réseau effective, communément appelée adresse IP. Ce service peut être vu comme une base de données distribuée dans l'Internet.

Le format des adresses défini dans le protocole IPv4 limite l'espace d'adressage à environ 4 milliards d'adresses IP. L'espace d'adressage sur Internet pourrait être rapidement saturé.

La recommandation RFC 3596 prend en compte le besoin d'augmenter cette capacité d'adressage ; il définit des extensions au DNS permettant d'intégrer le format et la dynamique de gestion des adresses IPv6. Cette RFC au statut « *Draft Standard* » est aujourd'hui implémentée dans toutes les solutions permettant de mettre en œuvre la résolution de noms.

Règle 07	DNS	IETF	
Pour accéder au service de résolution de noms de domaine, il est OBLIGATOIRE d'utiliser le service DNS.			

4.4.1.5. Sécurisation du service de nom de domaine

Le DNS est un service de base important permettant l'accès au réseau Internet. En effet, une requête vers un serveur fait appel quasi systématiquement à une résolution DNS, afin de transformer le nom du serveur en adresse IP, qui est la véritable information que comprennent les routeurs IP, afin de router les datagrammes IP entre eux.

Or le service DNS est l'un des moins sécurisés et ses diverses implémentations ont présenté par le passé de nombreuses vulnérabilités. Les service DNS, font également parfois l'objet de mauvaises installations et deviennent des vecteurs d'intrusion des SI.

Les attaques du DNS de type déni de service, usurpation ou inondation recensées par le SANS Institute ou les différents CERT sont nombreuses. De telles attaques, menées à grande échelle ou bien concentrées sur les serveurs racines de l'architecture hiérarchique du DNS peuvent, en quelques heures, paralyser l'utilisation du réseau.

Ce n'est que très récemment (au regard de l'apparition du DNS) que des extensions sécurité pour le DNS sont apparues. Ceci afin de sécuriser les échanges entre serveurs DNS, en permettant l'authentification des parties communicantes ainsi que l'intégrité des données échangées, grâce à l'utilisation de la signature numérique.

L'adoption de DNSsec (*DNS security extensions*) en tant que recommandation paraît aujourd'hui inévitable, son adoption sur le terrain prendra du temps. En attendant, de nombreux projets ont vu le jour afin d'expérimenter, d'améliorer puis de valider les fonctionnalités de DNSsec et préparer ainsi son futur déploiement à grande échelle.

En termes d'évolution des recommandations, les travaux portent essentiellement sur l'optimisation du support de DNSsec, que ce soit au niveau des performances (RFC 3226) ou au niveau de la facilité de mise en œuvre.

Recommandé	DNSsec	IETF	
Il est RECOMMANDE d'utiliser DNSsec pour la sécurisation d'un service de résolution de noms de domaine.			

4.4.1.6. Fédération d'identité

La fédération d'identité permet aux usagers d'accéder à différents services en ligne sur la base d'une authentification unique. Chaque autorité administrative conserve sa propre gestion de l'identification des usagers.

Une fédération d'identité repose sur les éléments suivants :

- un fournisseur de services : il offre des services à l'utilisateur et utilise le fournisseur d'identité pour l'authentification ;
- un fournisseur d'identité : il gère les informations relatives à l'identification et à l'authentification d'un usager ;
- le cercle de confiance : ensemble d'entités amenées à partager de l'information ; il est formé d'un portail s'appuyant sur un ou plusieurs fournisseurs d'identité ;
- une fédération d'identité : elle est une relation entre l'identité, le compte géré par le fournisseur d'identité et le compte géré par le fournisseur de services ; c'est l'utilisateur qui la construit en choisissant de fédérer/défédérer son compte avec les fournisseurs de services ; la relation entre les fournisseurs de services est matérialisée par un couple de clés de fédération connu uniquement par le fournisseur d'identité ;
- une clé de fédération : les différents fournisseurs de service ne peuvent communiquer directement entre eux à propos de l'identité d'un utilisateur ; ils ne peuvent échanger des informations le concernant qu'avec le fournisseur d'identité ; afin de garantir l'intégrité et la non-révocabilité de l'échange, un tiers de confiance, le fournisseur d'identités, émet un jeton de sécurité qui identifie la session mais pas l'utilisateur, ceci afin d'éviter la diffusion de ses données personnelles ;
- un utilisateur : il crée une fédération entre ses différents comptes ; il n'a besoin de s'authentifier qu'une seule fois pour accéder aux différents comptes fédérés.

Le consortium Liberty Alliance, soutenu par plus de 150 entreprises ou organismes internationaux, a spécifié le système d'authentification distribué ID-FF (*IDentity Federation Framework*). ID-FF permet à un utilisateur de disposer d'un compte différent sur plusieurs applications et de créer une fédération entre ces comptes. La spécification ID-FF 1.2 a été intégrée dans la recommandation d'assertion de sécurité SAML 2.0.

SAML (*Security Assertion Markup Language*) est un protocole de déclaration de données d'authentification et d'autorisation qui permet d'échanger des informations de sécurité.

Recommandé	SAML v2.0	OASIS - UIT	
Pour fédérer des services sur un cercle de confiance entre les administrations, il est RECOMMANDÉ d'utiliser le modèle de fédération supporté par la recommandation d'assertion de sécurité SAML 2.0.			

En observation	ID-WSF 2.0	Liberty Alliance	
Des principes complémentaires à ceux spécifiés dans SAML 2.0 décrivent le transport des attributs liés à l'identité. Ils sont spécifiés dans ID-WSF (Identity Web Service Framework).			

Les spécifications SAML et ID-WSF sont les plus répandues et les plus matures parmi les spécifications ouvertes sur la fédération d'identité. Il existe d'autres spécifications traitant de la fédération des identités comme [open ID](#) géré par l'Open ID Foundation ou [WS-Federation](#) basée sur la pile protocolaire WS-*

4.4.2. Technologies

4.4.2.1. Protocole réseau

Le protocole IPv4 se présente comme la référence des protocoles de niveau réseau pour l'interconnexion entre le réseau local Ethernet et les réseaux longue distance.

La version 4 du protocole IP est déployée universellement à travers le monde. Avec TCP, protocole de transport associé, IPv4 est le protocole de base du réseau Internet.

Règle 08	IPv4	IETF	
Pour l'ensemble des échanges au niveau de la couche réseau, il est OBLIGATOIRE d'utiliser le protocole IPv4.			

Ce protocole présente toutefois de nombreuses limites notamment :

- la capacité d'adressage, tant la croissance du réseau est importante (l'espace d'adressage devrait atteindre la saturation de 4 milliards d'adresses vers 2010),
- l'insuffisance des mécanismes de configuration d'adresse en termes de simplicité et d'automatisation, frein notable aux développements futurs du réseau Internet mobile,
- l'insuffisance des propriétés de qualité de service, notamment sur la priorité des flux temps réel,
- l'absence de fonctions intrinsèques de sécurité,
- l'absence de corrélation géographique dans le format d'adressage.

La version 6 du protocole IP apporte de nouvelles fonctionnalités pour résoudre certaines de ces limites. Il porte notamment la capacité du réseau internet à plus de 600 milliards d'adresses. L'évolution du marché décidera du moment opportun pour la migration IPv4 vers IPv6 (croissance du réseau, développement du réseau Internet mobile de masse, du multimédia, etc.).

Recommandé	IPv6	IETF	
Sur les équipements de cœur de réseau comme les serveurs, routeurs et commutateurs, il est RECOMMANDÉ de mettre en œuvre un système d'exploitation capable de gérer le protocole IPv6.			

La recommandation RFC 2675 propose la possibilité d'émettre des paquets de taille supérieure à 65 kilo-octets. Cette limite était jusqu'à maintenant établie par la conception des protocoles TCP/IP. Le dépassement de cette limite permet d'émettre de plus gros paquets sur les réseaux de type haut débit et d'accroître les performances aux nœuds d'interconnexion sur les transferts de données volumineux.

En effet, IPv6 permettant d'introduire des options de longueur variable au sein de l'en-tête de ses paquets, la limite des 65 kilo-octets de données n'est plus infranchissable. La recommandation RFC 2675 définit les conditions de mise en œuvre d'une option de dépassement de taille de paquets, ainsi que les améliorations à apporter aux protocoles TCP et UDP pour permettre cette évolution.

4.4.2.2. Protocoles de transport

Les protocoles TCP (*Transmission Control Protocol*) et UDP (*User Datagram Protocol*) forment, avec le protocole IP sous-jacent, le socle de base des protocoles de l'Internet.

De même que pour IP, ces protocoles n'ont pas beaucoup évolué depuis leurs spécifications initiales. De nombreuses options d'amélioration ont pourtant été définies mais elles ne sont actuellement pas suivies de manière homogène par le marché, de sorte que seules les fonctionnalités de base sont vraiment applicables.

Une recommandation, de référence RFC 1323, est toutefois relativement suivie. Elle propose des extensions d'amélioration de performance sur réseau haut débit. Ces extensions sont compatibles avec les applications distantes ne les supportant pas. La recommandation améliore la gestion de la fenêtre de transmission et la mesure du temps de transit.

Le protocole UDP est utilisé pour les transmissions de données en temps réel (flux multimédia, type Vidéoconférence, Voix sur IP, etc.). En effet, lors d'échanges en temps réel, les retransmissions de paquets perdus sont inutiles car les paquets retransmis arrivent trop tard. UDP étant plus simple, il permet donc d'aller plus vite.

Le protocole TCP reste le meilleur composant permettant de fiabiliser les flux de type HTTP, SMTP et FTP. Les fonctionnalités de retransmissions de TCP fiabilisent les échanges mais rendent ce protocole moins rapide que UDP.

Règle 09	TCP / UDP	IETF	 
Pour transporter les flux de données provenant des couches applicatives, il est OBLIGATOIRE d'utiliser les protocoles TCP ou UDP.			

Issu de travaux réalisés les acteurs télécoms, SCTP (*Stream Control Transport Protocol*) a pour objectif de répondre aux limitations de TCP en ajoutant les fonctionnalités suivantes : ordonnancement des paquets non-obligatoires en fonction des besoins, orientation message et non octet, rattachement multiple et amélioration de la sécurité.

En observation	SCTP	IETF	
Le protocole SCTP est à ce jour arrivé à maturité mais son adoption reste limitée. Une période d'observation est nécessaire.			

4.4.2.3. Protocole client-serveur

Le protocole HTTP (*HyperText Transfer Protocol*), littéralement « protocole de transfert hypertexte », est un protocole de communication informatique client-serveur développé pour le World Wide Web. Il est utilisé pour transférer les documents (document HTML, image, feuille de style, etc.) entre le serveur HTTP et le navigateur Web lorsqu'un visiteur consulte un site Web.

Règle 10	HTTP	IETF	
Pour la présentation et les échanges entre un serveur Web et un navigateur, il est OBLIGATOIRE d'utiliser le protocole HTTP 1.1.			

HTTPS est la combinaison du protocole HTTP et du service de sécurisation des échanges TLS.

-  Pour plus de détails sur TLS, se reporter au chapitre 4.4.2.8 *Service de sécurisation des échanges*

4.4.2.4. Accès aux ressources via HTTP

HTTP en version 1.1 définit officiellement 47 directives. La directive « *Allow* » définit les méthodes utilisées (GET, PUT, POST, ...) pour accéder aux ressources demandées.

Avec la méthode GET, le corps de message d'une requête http est vide.

Lorsque des informations sont envoyées au serveur à l'aide de la méthode GET, elles sont encodées à la suite de la ressource après le symbole « ? » dans l'URL.

La méthode POST est plus discrète. Elle permet d'envoyer des informations au serveur dans le corps du message d'une requête HTTP.

Recommandé	HTTP POST	W3C	
Lors du passage de paramètres à caractère confidentiel ou personnel, il est RECOMMANDÉ d'utiliser la méthode HTTP POST, au lieu de la méthode HTTP GET.			

La méthode GET devant garantir l'idempotence (les appels URL ne doivent pas provoquer de changement d'état du système), il est préférable d'utiliser la méthode POST pour les requêtes modifiant l'état du système, comme par exemple, un changement de mot de passe ou une création de compte.

Recommandé	HTTP POST	W3C	
Pour faire une requête provoquant un changement d'état persistant dans une application Web, il est RECOMMANDÉ d'utiliser la méthode HTTP POST.			

4.4.2.5. Meilleures pratiques HTTP

Encodage de caractères

Lors d'une transaction entre un serveur web et un navigateur, le serveur web renseigne l'attribut « Content-Type ». Il précise ainsi au navigateur le type du fichier envoyé, afin que celui-ci affiche le document dans le format attendu.

Règle 11	HTTP Content Type	IETF	
Il est OBLIGATOIRE de renseigner l'attribut "Content-Type" du protocole http.			

Compression

La compression HTTP est paramétrable au niveau des serveurs web et permet des gains en bande passante.

Recommandé	HTTP	IETF	
Il est RECOMMANDÉ d'activer la compression HTTP au niveau des serveurs web.			

Gestion du cache mémoire

Il est possible d'imposer aux applications de gérer le cache des pages qu'elles diffusent, en utilisant le paramètre Cache-Control du protocole HTTP/1.1 (se reporter à la section 13 et 14 de la recommandation RFC 2616) ainsi que le paramètre Last-Modified.

Un serveur diffusant des **articles de communication** précisera :

- "Cache-Control: public",
- "Last-Modified: Dernière date de modification",
- "Expires: Date de prochaine validation par le cache"(si possible).

Un serveur manipulant des données à **caractère personnel et/ou confidentiel** précisera :

- "Cache-Control: private".

Ainsi, un serveur peut éditer des pages sensibles mais dont les logos et images ne le sont pas. Ces composants seront mis en cache mémoire, ce qui permettra de réaliser une économie de bande passante. Inversement, un serveur diffusant des images à caractère confidentiel les fera précéder de "Cache-Control: private". Les bonnes pratiques consistent donc à renseigner l'en-tête avec :

- "Cache-Control" du protocole HTTP/1.1 pour les pages dynamiques diffusées par HTTP,
- "Last-Modified" du protocole HTTP/1.1 pour les pages dynamiques diffusées par HTTP et dont le cache est autorisé par l'en-tête "Cache-Control: public",
- "Expires" du protocole HTTP/1.1 pour les pages dynamiques diffusées par HTTP et dont le cache est autorisé par l'en-tête "Cache-Control: public".

4.4.2.6. Services de transfert de fichiers

Communément, le transfert de fichiers entre deux ordinateurs connectés à un réseau IP s'effectue via le protocole FTP (*File Transfer Protocol*). D'utilisation simple, ce protocole a prouvé son efficacité en matière de transfert de gros volumes de données.

Ce protocole FTP s'est étoffé grâce aux nouvelles extensions :

- de sécurité (RFC 2228 et 2773),
- d'internationalisation et de prise en compte du codage UTF-8 (RFC 2640).

Des extensions FTP sont prévues pour interopérer avec le protocole IPv6.

Le protocole SFTP (SSH File Transfer Protocol) est un protocole sécurisé pour transférer des fichiers à distance de manière sécurisée.

Recommandé	FTP	IETF	
Pour transférer des fichiers, il est RECOMMANDÉ, hors contexte Web, d'utiliser le protocole SFTP ou à défaut le protocole FTP.			

En contexte web, HTTP sera préféré à FTP pour le transfert de fichiers.

4.4.2.7. Sécurisation du protocole réseau

IPsec (*Internet Protocol security*) est un protocole qui assure l'authentification, le chiffrement des données et l'intégrité. Conçu à l'origine pour IPv6, IPsec a été adapté pour fonctionner avec IPv4.

Contrairement à TLS qui est spécifié au niveau de la couche présentation, IPsec est définie au niveau IP (couche réseau). Il permet par exemple de réaliser des VPN (*Virtual Private Network* ou réseau privé virtuel).

Un réseau privé virtuel construit avec la technologie IPsec consiste à établir deux canaux de communication (des tunnels) entre les machines :

- un canal d'échange de clés, sur une connexion UDP depuis et vers le port 500 : ISAKMP (*Internet Security Association and Key Management Protocol*),
- un ou plusieurs canaux de données par lesquels le trafic du réseau privé est véhiculé selon les deux protocoles possibles suivants :
 - ESP (*Encapsulating Security Payload*), qui fournit l'intégrité et la confidentialité,
 - AH (*Authentication Header*) qui ne fournit que l'intégrité.

La mise en œuvre du protocole IPsec se fait généralement au niveau des routeurs. Ces équipements permettent en effet d'optimiser les paramètres liés à la couche réseau.

Recommandé	IPsec	IETF	
Il est RECOMMANDÉ d'utiliser le protocole IPsec au niveau de la couche réseau, pour chiffrer, authentifier et valider l'intégrité des échanges.			

4.4.2.8. Service de sécurisation des échanges

TLS (*Transport Layer Security*) est un protocole de sécurisation des échanges sur Internet.

Développé à l'origine par la société Netscape, anciennement nommé SSL (*Secure Socket Layer*), il a été renommé TLS suite au rachat du brevet par l'IETF en 2001.

TLS fonctionne suivant un mode client-serveur. Il répond aux quatre mesures de sécurité suivantes :

- authentification du serveur,
- confidentialité des données échangées (ou session chiffrée),
- intégrité des données échangées,
- authentification du client, de manière optionnelle.

Dans la pile protocolaire, TLS se situe entre les couches applications (comme HTTP, FTP, SMTP) et la couche transport TCP. Son utilisation la plus commune reste cependant au dessous de HTTP. La couche TLS est implémentée par la couche application de la pile, ce qui a deux conséquences :

- pour toute application existante, il peut exister une application utilisant TLS. Par exemple, l'application HTTPS correspond à HTTP au dessus de TLS ;
- une application TLS se voit attribuer un nouveau numéro de port par l'IANA (*Internet Assigned Numbers Authority*). Par exemple HTTPS est associé au port 443.

Règle 12	TLS	IETF	
Pour sécuriser les échanges s'appuyant sur des protocoles applicatifs (FTP, HTTP, IMAP, LDAP, POP3, SIP, SMTP, etc.), il est OBLIGATOIRE d'utiliser le protocole TLS ou SSL V3.0.			

4.4.2.9. Diffusion vidéo en mode continu

La diffusion vidéo en mode continu (*Streaming Video*) est une technique qui permet de faire circuler sur un réseau à protocole IP (un intranet, un extranet ou le réseau Internet), des flux de données contenant des séquences audio ou vidéo.

Cette technique est différente de la diffusion en mode téléchargement, qui nécessite de récupérer l'ensemble des données d'une séquence audio ou vidéo, avant de pouvoir l'exploiter.

Les transmissions et la communication entre serveur et client peuvent utiliser les protocoles RTP ou RTSP (protocoles normalisés par l'IETF). Se reporter au chapitre consacré à la téléphonie pour obtenir des précisions sur ces protocoles.

Recommandé	RTP / RTSP	IETF	
Il est RECOMMANDE d'utiliser RTP ou RTSP pour la diffusion de vidéo en mode continu.			

-  Des problèmes d'interopérabilité peuvent apparaître selon les codecs vidéo choisis pour les médias faisant l'objet de la diffusion en mode continu. Se référer aux thèmes 3.1.5 *Formats de séquence vidéo*

4.4.2.10. Horodatage et synchronisation

4.4.2.10.1. Synchronisation des horloges

Le protocole NTP (*Network Time Protocol*) permet de synchroniser l'horloge d'un ordinateur avec celle d'un serveur de référence. NTP est un protocole basé sur une couche de transport UDP.

Le protocole SNTP (*Simple Network Time Protocol*) est une adaptation simplifiée de NTP.

Règle 13	NTP	IETF	
Pour réaliser une synchronisation des horloges des différents ordinateurs et équipements réseaux constituant un SI, il est OBLIGATOIRE d'utiliser le protocole NTP.			

4.4.2.10.2. Horodatage technique

TDF (Télé Diffusion de France) et DCF77 sont des systèmes de transmission de l'heure légale par ondes radio, sur une large zone de couverture.

Recommandé	Signaux horaires (France Métropolitaine)
Il est RECOMMANDÉ d'utiliser les signaux horaires TDF (162 kHz) ou DCF77 (77,5 kHz) pour d'obtenir une fonction d'horodatage technique précise.	

Pour les zones géographiques situées en Outre-mer (les DOM et les TOM), la mise en œuvre de système utilisant la réception de signaux horaires provenant de satellites GPS, ou des futurs satellites Galiléo, est recommandée.

4.4.2.10.3. Temps UTC ou TAI

Il est intéressant de préciser si les serveurs de temps mis à disposition doivent transmettre une heure UTC (Temps Universel Coordonné) ou TAI (Temps Atomique International).

UTC est une échelle de temps adoptée comme base du temps civil international par un grand nombre de pays. C'est un compromis entre le TAI, stable mais déconnecté de la rotation de la Terre et le temps universel TU, directement lié à la rotation de la Terre mais instable.

L'utilisation du format de fréquence UTC est proposée par l'UIT-R (Union Internationale des Télécommunications- secteur des radio-communications) comme référence dans les émissions de fréquences étalon et de signaux horaires.

Recommandé	UTC	UIT-R	
Il est RECOMMANDÉ que les serveurs de temps mis à disposition des SI, transmettent une heure au format UTC.			

5. Glossaire

Des termes en langue anglaise sont parfois maintenus ou mis en complément entre parenthèses dans le présent document. Ceci permet de ne pas introduire de doute ou d'ambiguïté sur le sens du terme employé.

Terme	Description
AFNOR	Association Française de Normalisation
Agent	Personne physique agissant pour le compte d'une autorité administrative.
ANSI	American National Standards Institute
Autorité Administrative	Sont considérées comme autorités administratives les administrations de l'Etat, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes de protection sociale relevant du code de la sécurité sociale et du code rural ou mentionnés aux articles L.223-16 et L.351-21 du code du travail et les autres organismes chargés de la gestion d'un public administratif.
BAL	Boîte Aux Lettres
BPMI	Business Process Management Initiative
BPMN	Business Process Modelling Notation
BRS	Business Requirements Specification – Spécification des exigences métier
CAMSS	Common Assessment Method for Standards and Specifications
CCL	UN/CEFACT Core Component Library – Bibliothèque de composants communs du CEFACT/ONU
CCTS	Core Component Technical Specification – Spécification technique des composants communs
CEI	Commission Electrotechnique Internationale
CEN	Comité Européen de Normalisation
CEN/ISSS	CEN/Information Society Standardization System
CENELEC	Comité européen de normalisation électrotechnique
CGM	Computer Graphics Metafiles
CNIL	Commission Nationale de l'Informatique et des Libertés
CNIS	Chinese National Institution of Standardization
Concept	Idee, objet conçu par l'esprit ou acquis par lui et permettant d'organiser les perceptions et les connaissances

Terme	Description
CSS	Cascading Style Sheet
CSV	Comma Separated Value
DGME	Direction Générale de la Modernisation de l'Etat (Ministère du Budget)
Domaine d'interopérabilité	Les niveaux d'interopérabilité du RGI sont subdivisés de domaines. Par exemple, les domaines Multimédia ou Présentation sont des domaines du niveau technique. Ils peuvent être divisés en sous-domaines
DNG	Digital Negative
DNS	Domain Name System
DNSsec	Domain Name System Security Extension
DWG	DraWinG
ECMA	Ecma International – European association for standardizing information and communication systems
EDI	Electronic Data Interchange
EIF	European Interoperability Framework
EPS	European Public Services
ESMTP	Extended Simple Mail Transfer Protocol
ETSI	European Telecommunications Standards Institute Institut européen des normes de télécommunication
FTP	File Transfer Protocol
HL7	Health Level 7
HTML	HyperText Markup Language
HTTP	HyperText Transfert Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IDABC	Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens
IEC	International Electrotechnical Commission
CEI	Commission Electrotechnique Internationale
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
iLBC	Internet Low Bit rate Codec
IMAP	Internet Message Access Protocol
INCITS	InterNational Committee for Information Technology Standards
INSEE	Institut National de la Statistique et des Études Économiques
Interopérabilité	La capacité d'un système à fonctionner avec d'autres systèmes

Terme	Description
IP	Internet Protocol
IPsec	Internet Protocol Security
ISO	International Organization for Standardization Organisation internationale de normalisation
JPEG	Joint Photographic Experts Group
JO	Journal Officiel
JSON	JavaScript Object Notation
JSR 168	Java Specification Requests : Portlet Specification
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Data Interchange Format
MDC	Modèle de Données Communes
Métadonnée	Donnée servant à définir ou décrire une autre donnée
Méthode	Démarche organisée rationnellement pour aboutir à un résultat
MIME	Multipurpose Internet Mail Extensions
Modèle	Plan, représentation ou description conçu pour décrire un objet, un système ou d'une manière générale une vision de la réalité
MPEG	Moving Picture Experts Group
NASA	National Aeronautics and Space Administration
NIFO	National Interoperability Framework Observatory
NIST	National Institute of Standards and Technology
Niveau d'interopérabilité	Les échanges entre parties prenantes reposent sur 6 niveaux d'interopérabilité : les niveaux politique, juridique, organisationnel, sémantique, syntaxique, technique. Le RGI traite des trois derniers niveaux
Nomenclature	Catalogue, répertoire ou liste détaillés dans lesquels sont définis et classés des éléments ayant trait à un sujet donné et auxquels on peut se référer
Norme	Document de référence fixant les conditions dans lesquelles une opération est réalisée, un objet exécuté, un produit élaboré, avec deux caractéristiques fondamentales: <ul style="list-style-type: none"> être à la fois le fruit du consensus de l'ensemble des acteurs et le résultat du transfert du savoir-faire de ces acteurs, émaner des organismes officiels de normalisation.
NTP	Network Time Protocol
OASIS	Organization for the Advancement of Structured Information Standards
OCL	Object Constraint Language
ODF	Open Office Document
OMG	Object Management Group

Terme	Description
OXML	Office Open XML
Partie prenante	Tout acteur, personne physique ou entité technique, participant à un échange par voie électronique
PCM	Pulse Code Modulation
PDF	Portable Document Format
PNG	Portable Network Graphics
POP	Post Office Protocol
Praxeme	Méthode de modélisation d'entreprise et de conception du SI
PRESTO	PRotocol d'Echanges STandard et Ouvert
Processus	Ensemble d'activités corrélées ou interactives qui transforme des éléments d'entrée en éléments de sortie.
RDF	Resource Description Framework
REST	Representational State Transfer
RGAA	Référentiel Général d'Accessibilité pour les Administrations
RGI	Référentiel Général d'Interopérabilité
RGS	Référentiel Général de Sécurité
RPC	Remote Procedure Call
RSM	Requirements Specification Mapping
RSS	Really Simple Syndication
RTCP	Real-time Transport Control Protocol
RTP	Real-Time Transport Protocol
RTSP	Real-Time Streaming Protocol
S/MIME	Secure / Multipurpose Internet Mail Extensions
SAML	Security Assertion Markup Language
SCTP	Stream Control Transmission Protocol
Sémantique	La sémantique recouvre à la fois la signification des mots et le rapport entre le sens des mots (homonymie, synonymie, etc.)
Service en ligne	Tout SI permettant aux usagers de procéder par voie électronique à des démarches ou formalités administratives. Egalement appelé téléservice
SFTP	Secure File Transfert Protocol
SI	Système d'information
SIP	Session Initiation Protocol
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol

Terme	Description
SOAP	Simple Object Access Protocol
SSL	Secure Sockets Layer
Standard	Modèle de référence adopté par l'usage d'un groupe de personnes
SVG	Scalable Vector Graphics
Système d'information	Tout ensemble de moyens destinés à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives
TCP	Transmission Control Protocol
TDF	TéléDiffusion de France
TIFF	Tagged Image File Format
TLS	Transport Layer Security
ToIP	Telephony over Internet Protocol
UDDI	Universal Description Discovery and Integration
UDP	User Datagram Protocol
UIT	Union Internationale des Télécommunications
UIT-T	Section de l'UIT dédiée à la normalisation
UML	Unified Modeling Language - Langage de modélisation unifié
UMM	UN/CEFACT Modeling Methodology – Méthodologie de modélisation du CEFACT-ONU
UN	United Nations
ONU	Organisation des Nations Unies
UN/CEFACT	United Nations Centre for Trade Facilitation and Electronic Business ou Centre des Nations Unies pour la facilitation du commerce et les transactions électroniques
UN/EDIFACT	United Nations / Electronic Data Interchange for Administration Commerce and Transport
Usager	Personne physique agissant pour son propre compte ou pour le compte d'une personne morale et procédant à des échanges électroniques avec des autorités administratives
UTC	Temps Universel Coordonné
UTF-8	8-bit Unicode Transformation Format
VoIP	Voice over Internet Protocol
W3C	World Wide Web Consortium
WAI	Web Accessibility Initiative
WAV	Waveform audio format
WS-I	Web Services Interoperability Organisation
WSDL	Web Services Description Language

Terme	Description
WSRP	Web Services for Remote Portlets
WSS	Web Service Security
X3D	Extensible 3D
XHTML	Extensible Hypertext Markup Language
XMI	XML Metadata Interchange
XML	eXtensible Markup Language – Langage de balise extensible
XML NDR	XML Naming and Design Rules – Règles de nommage et de conception XML
XMPP	eXtensible Messaging and Presence Protocol
XPath	XML Path Language
XSD	XML Schema Definition
XSLT	Extensible Stylesheet Language Transformation

6. Gestion des versions

Version	Date	Description
0.99d	14-04-2009	Refonte des trois volets organisationnel, sémantique et technique en un seul document. Articulation avec les autres référentiels. Ajout du cadre d'interopérabilité. Revue sur les règles existantes.
1.0	12-05-2009	Projet final pour avis

7. Sommaire détaillé

ORGANISATION DU DOCUMENT	2
AVANT-PROPOS	3
LE DEFAUT D'INTEROPERABILITE	3
COMMENT RESOUDRE UN DEFAUT D'INTEROPERABILITE ?	3
UN REFERENTIEL D'INTEROPERABILITE POUR LES SYSTEMES D'INFORMATION	3
LES DIX BENEFICES ATTENDUS DU RGI	4
PRECISIONS IMPORTANTES	7
PARTIE 1 : CADRE D'INTEROPERABILITE	8
SOMMAIRE DU CADRE D'INTEROPERABILITE	9
1. CONTEXTE ET ENVIRONNEMENT	10
1.1. L'ADMINISTRATION EN LIGNE	10
1.2. CADRE LEGISLATIF	10
2. DEMARCHE D'ELABORATION	11
2.1. DEMARCHE ET PARTIS PRIS.....	11
2.2. DEMARCHE DE SELECTION DES NORMES ET STANDARDS	12
2.2.1. Normes et standards	12
2.2.2. Critères d'adoption retenus.....	12
2.3. ORGANISMES DE NORMALISATION	14
3. DOMAINES D'INTEROPERABILITE	15
3.1. PERIMETRE DE L'INTEROPERABILITE.....	15
3.2. TYPOLOGIE DES ACTEURS CONCERNES	16
4. PRESENTATION DES NIVEAUX D'INTEROPERABILITE	17
4.1. LES DIFFERENTS NIVEAUX D'INTEROPERABILITE	17
4.2. LES NIVEAUX D'INTEROPERABILITE TRAITES PAR LE RGI.....	18
4.2.1. Les domaines de l'interopérabilité sémantique	19
4.2.2. Les domaines de l'interopérabilité syntaxique.....	19
4.2.3. Les domaines de l'interopérabilité technique.....	19
5. EVOLUTION DU DOCUMENT	20
6. MODALITES D'APPLICATION DU RGI	21
PARTIE 2 : GUIDE D'INTEROPERABILITE	22
SOMMAIRE DU GUIDE D'INTEROPERABILITE	23
1. STRUCTURE DU GUIDE D'INTEROPERABILITE	24
1.1. GUIDE D'INTEROPERABILITE	24
1.2. PRESENTATION DES REGLES D'INTEROPERABILITE	25
1.3. LISTE DES NORMES ET STANDARDS REFERENCES	26
2. INTEROPERABILITE SEMANTIQUE	27
2.1. INTRODUCTION	27
2.2. CONCEPTION DES ECHANGES	29
2.2.1. Les concepts de base liés aux échanges.....	29
2.2.2. Une démarche générique de conception des échanges.....	30
2.3. METHODES DE SPECIFICATION ET LANGAGES	35
2.3.1. Méthodes de spécification	35
2.3.2. Des langages pour décrire les échanges.....	37
2.4. REUTILISATION DES RESSOURCES SEMANTIQUES.....	41

2.4.1.	<i>Ressources communes aux échanges</i>	41
2.4.2.	<i>Ressources pour l'archivage</i>	46
3.	INTEROPERABILITE SYNTAXIQUE	50
3.1.	FORMATS ELEMENTAIRES.....	51
3.1.1.	<i>Codage des caractères</i>	51
3.1.2.	<i>Polices d'écriture</i>	52
3.1.3.	<i>Formats d'image</i>	53
3.1.4.	<i>Formats de séquence sonore</i>	54
3.1.5.	<i>Formats de séquence vidéo</i>	55
3.1.6.	<i>Formats d'objet graphique en 2D</i>	56
3.1.7.	<i>Formats d'objet et d'univers 3D</i>	57
3.1.8.	<i>Formats de dessin technique</i>	58
3.1.9.	<i>Exportation de bases de données</i>	59
3.2.	FORMATS COMPOSITES.....	60
3.2.1.	<i>Echange de documents bureautiques révisables</i>	61
3.2.2.	<i>Echange de documents bureautiques non révisables</i>	62
3.2.3.	<i>Archivage de documents bureautiques non révisables statiques</i>	63
3.2.4.	<i>Conservation des documents bureautiques dynamiques</i>	64
3.2.5.	<i>Echange de données numériques d'impression</i>	65
3.2.6.	<i>Echange de documents structurés</i>	66
3.2.7.	<i>Langage de transformation de données structurées</i>	67
3.2.8.	<i>Service de compression de fichiers</i>	68
3.2.9.	<i>Syndication de contenu</i>	69
4.	INTEROPERABILITE TECHNIQUE	70
4.1.	PRESENTATION.....	71
4.1.1.	<i>Technologies pour construire les IHM</i>	71
4.1.2.	<i>Feuilles de styles</i>	72
4.1.3.	<i>Utilisation de scripts</i>	73
4.1.4.	<i>Navigateurs web</i>	74
4.2.	MULTIMEDIA.....	75
4.2.1.	<i>Messagerie</i>	75
4.2.2.	<i>Téléphonie</i>	80
4.3.	SERVICES WEB.....	86
4.3.1.	<i>Protocole d'échange des messages de l'administration</i>	87
4.3.2.	<i>Les Services Web SOAP</i>	88
4.3.3.	<i>Les Services Web REST</i>	94
4.4.	INFRASTRUCTURE.....	95
4.4.1.	<i>Services d'annuaires et fédération d'identité</i>	95
4.4.2.	<i>Technologies</i>	101
5.	GLOSSAIRE	111
6.	GESTION DES VERSIONS	117
7.	SOMMAIRE DETAILLE	118