



A1 - Tenir compte du caractère évolutif des TIC

Auteurs :

Fernand ETTORI
Université de Corse

Marcela MAFTOUL
Université de Grenoble II

Bernard PELLEFIGUE
Université de Toulouse II

Thierry SPRIET
Université d'Avignon et des Pays de Vaucluse

Module développé dans le cadre du projet C2IMES 2005,
Certification Informatique et Internet
Mutualisée pour l'Enseignement Supérieur

Edition : C2IMES, www.c2imes.org

Scénarisateur : Angélique Froger

Version : 1.0



Publié sous licence Creative Commons "By-NonCommercial-ShareAlike"
- <http://creativecommons.org/licenses/by-nc-sa/2.0/> -
Remarque importante : "Vous n'avez pas le droit d'utiliser ce document à des fins
commerciales sans l'autorisation préalable de l'auteur"



Table des matières

 Présentation du module et des objectifs pédagogiques.....	5
---	---

Chapitre I. Les TIC : définitions et obsolescences..... 7

A. Définition : les Technologies l'Information et de la Communication.....	7
B. L'information privée et personnelle : un matériel toujours obsolètes ?...	8
C. Obsolescences des connaissances en informatique ?.....	11
D. Les acteurs de l'Internet public.....	12

Chapitre II. Travailler dans un esprit d'ouverture et d'adaptabilité..... 13

A. Qu'est-ce qu'un logiciel ?.....	14
Partie A. Les licences des logiciels.....	15
1. Le contenu des licences.....	15
2. Les types de licence.....	16
Partie B. Les logiciels libres.....	17
 Exercice n°1. Que savez-vous des logiciels libres ?.....	17
1. Historique : Au début, il y avait Stallman.....	17
2. Les 4 libertés du logiciel libre.....	19
3. Coût du logiciel libre.....	19
4. Galerie non-exhaustive de logiciels libres.....	20
B. Connaître les règles de création et d'échange.....	23
C. Quelques ressources consultée lors de la rédaction de ce chapitre.....	24
 Synthèse.....	24

Chapitre III. La tour de Babel des systèmes d'exploitation, des normes et des standars..... 25

 Préambule.....	25
A. L'interopérabilité.....	27

B. Les normes ouvertes et communautaires.....	29
C. Les formats fermés et propriétaires.....	30
D. Entre les deux : les normes à distribution restreinte.....	31
E. Relation entre l'informatique et l'interopérabilité.....	31
F. Interopérabilité en bureautique.....	31

Chapitre IV. Les formats de fichiers ouverts pour l'échange de l'information.....35

A. Formats des images fixes et des animations.....	36
B. Formats pour le son et la vidéo.....	38
C. Formats pour les documents non structurés et semi-structurés (traitement de texte, tableur, présentation).....	40
D. En pratique.....	41
E. Pour en savoir plus.....	43

Conclusion..... 45

Annexes.....	53
---------------------	-----------

Présentation du module et des objectifs pédagogiques

Introduction

Ce module, très court, est un module transversal sur certaines questions générales que l'on doit se poser autour de l'utilisation des Nouvelles Technologies de l'Information et de la Communication actuellement.

Dans ce module, vous trouverez donc des réponses aux questions suivantes :

- ◆ Que sont les NTIC ?
- ◆ Qu'en est-il de l'évolution extrêmement rapide du matériel informatique et des usages associés ?
- ◆ Que pourra être notre société informatique dans 20 ans ?
- ◆ Un logiciel, c'est quoi exactement ?
- ◆ L'obsolescence rapide du matériel informatique, est-ce un mythe, une réalité ?
- ◆ Vos apprentissages d'aujourd'hui vous seront-ils utiles dans quelques années et à quelles conditions ?
- ◆ Comment naviguer entre les normes et les formats compatibles pour pouvoir toujours envoyer un document lisible quel que soit son destinataire ?

Les TIC : définitions et obsolescences

A. Définition : les Technologies l'Information et de la Communication

Dans les années 1990, on parlait plutôt des *NTI*, *Nouvelles Technologies de l'Information*, mais avec le mariage de l'informatique, de l'électronique, des télécommunications et de l'audiovisuel, on préfère parler désormais des *NTIC* : *Nouvelles Technologies de l'Information et de la Communication* qui restent dans l'esprit du grand public associé à l'usage d'informatique connecté à internet.

On remarquera que beaucoup de chercheurs et praticiens demandent à supprimer le terme nouveau en remplaçant *NTIC* par *TIC*, en expliquant qu'on ne peut pas éternellement désigner comme nouvelles des techniques qui sont maintenant pour certaines d'entre elles utilisées depuis 40 ans.

Mais comme dans l'esprit du grand public, parler de *NTIC* permet d'écartier les techniques de l'image et du son pour recentrer sur l'informatique et ses usages, on gardera le terme de *NTIC*.

B. L'information privée et personnelle : un matériel toujours obsolètes ?

D'avantage que dans les autres secteurs industriels, l'industrie informatique pousse au renouvellement rapide de ses produits.

Déjà ce secteur a réussi depuis près de 40 ans à multiplier constamment la puissance du matériel informatique à prix constant, ceci en suivant ce qu'on a appelé « *la loi de Moore* » (voir encarté).

Les constructeurs communiquent sur des nouvelles gammes de produits [Imprimantes, processeurs, cartes graphiques, ...] pratiquement tous les trimestres et tout est fait, poussé par l'industrie du jeu vidéo sur ordinateur, pour amener les particuliers et les entreprises à changer le plus souvent possible leur équipement informatique.



Conseil

Pourtant, il est bon de rappeler certaines évidences :

- ◆ Quand vous achetez du matériel informatique à une date donnée, tout ce que ce matériel peut réaliser : par exemple de la bureautique, du traitement vidéo ou audio, regarder des films, jouer, communiquer par mail , il pourra le réaliser durant toute sa durée de vie.
 - Il faut donc faire attention à la notion d'obsolescence du matériel informatique.
- ◆ Il apparaît juste de temps en temps des nouveaux logiciels, plus gourmands en ressources matérielles [Ressources matérielles qui demandent donc plus de mémoire, des processeurs plus puissants, un plus gros disque dur.] qui, eux, ne fonctionneront plus sur votre ordinateur.
 - Mais tous les logiciels que vous faisiez tourner sur votre équipement fonctionneront bien évidemment sur celui-ci 10 ans après si votre matériel marche toujours.
- ◆ Aussi attention à ne pas trop prêter attention aux discours industriels qui vous incitent plus souvent que de raison à renouveler votre matériel là ou un simple rajout de disque dur ou de mémoire suffirait à poursuivre son utilisation pour des usages nouveaux et où rien n'est nécessaire pour poursuivre vos usages habituels.

Et nous vous recommandons la lecture attentive du *BI* pour votre choix de matériel informatique.



La loi de Moore

Exprimée en 1965 puis reformulé en 1975 par *Gordon Moore*, ingénieur cofondateur d'Intel, la "*Loi de Moore*" (qui n'est pas une loi physique mais juste une prévision qui s'est révélée exacte) annonçait *un doublement du nombre de transistors sur une puce tous les 24 mois*.

Elle a fêté ses 40 ans il y a peu et reste d'actualité alors que dans les années 60 on ne mettait avec peine que 30 transistors sur une puce et qu'aujourd'hui les transistors se comptent en dizaines de millions et leurs tailles s'expriment en nanomètres.



Quel matériel pour quels usages ?

À part pour des usages spécifiques[Principalement le jeu 3D, le traitement vidéo et audio les ordinateurs.], même relativement anciens[Moins de 7 ans.]peuvent pratiquement tous faire de la bureautique[Traitement de texte, tableur, présentation, ...], de la navigation et mail sur Internet[La lenteur des connections peut venir de votre débit de connexion ,elle ne viendra pas de votre équipement informatique.]et du visionnage de film.

Un peu de futurologie ...

Ces prospections sont fortement inspirées d'un rapport du cabinet *Prosodie*, groupe international d'experts en informatique, qui a tenté en 2006 avec un certain nombre de spécialistes d'imaginer ce que sera l'informatique de demain.

Attention, la plupart du temps ce type de prévisions sous-estiment certaines évolutions et sur-estiment d'autres changements qui n'ont en fait jamais lieu ce qui n'empêche pas leurs intérêts prédictifs.

Si on se penche sur l'évolution passée de l'informatique et qu'on tente de prévoir comment seront constitués les équipements informatiques et les usages de demain (en 2027)...

◆ Puissance informatique

La puissance informatique des équipements devrait être multipliée par 8 000 à coût constant. Là en lisant ce module, vous utilisez probablement un ordinateur dont la puissance de calcul ridiculiserait celui de la Nasa qui en 1969 a envoyé des hommes sur la lune. Pourtant cet ordinateur sera considéré comme une calculatrice-jouet par les usagers de l'informatique en 2027. Paradoxalement cet ordinateur de 2027 ne sera pas encore capable de réaliser, en terme de puissance de calcul, ce qu'un cerveau humain peut réaliser.

Par contre, on verra probablement éclore grâce à cette puissance de plus en plus de logiciels simulant vocalement, graphiquement et en terme de contenu des personnes humaines. Ainsi, nous aurons des sortes d'interlocuteurs virtuels qui répondront à nos questions quand on aura un problème de livraison de colis par la Poste, par exemple.

◆ Nombres d'internautes et identités virtuelles

En 2027, on table sur 3 milliards d'utilisateurs d'Internet et quelques dizaines de milliards de « pseudos », sorte d'identités virtuelles déclarées qui permettent à chaque internaute d'utiliser différentes identités selon des besoins spécifiques (privés, professionnels, etc.).

◆ Accès au réseau Internet

On disposera probablement presque tous d'un accès réseau avoisinant les 100 téraoctets par secondes (pour infos, les connections adsl sont aujourd'hui plutôt de 1 à 16 mégabits par secondes) soit 12500 fois plus rapide ce qui permettrait donc des usages de vidéos hautes définitions instantanément et transformerait complètement la notion d'échanges de fichiers.

Aujourd'hui 1,3 milliard de terminaux mobiles sont connectés à Internet parmi eux principalement des ordinateurs mais également des PDA (personal digital assistant) et des téléphones portables.

En 2027 on peut estimer que 40 milliards d'outils divers seront connectés à Internet, avec de plus en plus d'électronique connectée et intégrée dans toutes les machines que nous utilisons[Bien sûr tous les ordinateurs et portables seront connectés mais aussi des portails de maison, réfrigérateurs, machines à

café, montres, etc.].

◆ Usages logiciels

Enfin, en termes d'usages logiciels, il est extrêmement difficile de prévoir les évolutions, probablement de moins en moins de logiciels installés sur nos machines et plutôt des applications disponibles sur le réseau. Par contre, nul ne peut prévoir si des logiciels de traduction simultanés seront enfin opérationnels à cette date, avec toute la révolution que cela induirait.

C. Obsolescences des connaissances en informatique ?

Dans les passages précédents, on a vu qu'il fallait prendre du recul sur l'évolution rapide du matériel informatique et sa relative obsolescence.

Pourtant il existe un domaine où l'obsolescence est manifeste et où il faut impérativement actualiser ses compétences le plus souvent possible, c'est justement l'informatique.

Pour cela, par exemple, comprendre le fonctionnement des *flux RSS* décrit dans le module *B7* permet à chacun d'entre nous, en y consacrant un temps limité de garder un bon niveau de maîtrise sur tous les changements intéressants qui se produisent dans sa branche.

Et également de continuer à se former aux nouveaux outils informatiques et logiciels que vous avez appris pendant vos études.



Exemple

Un étudiant qui a passé son Certificat *C2I* avec succès en 2004 saura probablement toute sa vie bien structurer un document avec un traitement de texte ou utiliser un tableur s'il continue à pratiquer ces outils.

Cependant ce même étudiant n'aura pas appris par exemple ce qu'est un flux RSS car ce n'était pas demandé dans le référentiel du *C2I* en 2004.

Il est donc important de comprendre que les connaissances que vous obtenez aujourd'hui d'utilisation d'outils informatiques correspondent à une date millésimée.

Il sera de votre ressort ensuite d'actualiser ces connaissances pour pouvoir bénéficier d'usages plus pertinents qui se développeront ou de nouvelles possibilités offertes par des nouveaux logiciels par exemple.

D. Les acteurs de l'Internet public

Créé en 1998, le *Comité Interministériel pour la Société de l'Information (CISI)* définit les grandes orientations politiques et les priorités d'action pour l'intégration et le développement des nouvelles technologies.

Il évalue les initiatives mises en oeuvre et l'état de développement de la société de l'information.

Il intervient sur les questions techniques, sociales et juridiques liées aux TIC.

Chaque CISI comporte une dominante thématique :

- ◆ Entrée de la France dans la société de l'information (1998) ;
- ◆ Administration électronique et fondements d'une société de l'information solidaire (1999) ;
- ◆ Effort public de recherche (2000).



Présentation des acteurs de l'Internet public

- ◆ *Internet.gouv.fr* - Le portail société de l'information
 - <http://www.internet.gouv.fr/acteurs/> [<http://www.internet.gouv.fr/acteurs/>]

Travailler dans un esprit d'ouverture et d'adaptabilité

Ce chapitre présente les conditions permettant de travailler dans un esprit d'ouverture et d'adaptabilité. Il explique la notion du logiciel et ses différentes licences.

Il s'attache ensuite à expliquer l'historique et les principes du logiciel libre dont la caractéristique principale est justement l'ouverture du code source et qui seul garantit la facilité des échanges. Vous verrez à la fin que les textes officiels récents de l'État français soutiennent cette approche.

Temps d'apprentissage :

- ◆ 30 minutes (ou plus si on approfondit par la lecture des ressources proposées).

A. Qu'est-ce qu'un logiciel ?

Quelques définitions de base



Logiciel

Du point de vue de l'utilisateur, un logiciel est une application qui répond à l'un de ses besoins. C'est une suite d'instructions écrites dans un des langages informatiques qui forme un tout cohérent.

Selon Wikipedia [<http://fr.wikipedia.org/wiki/Logiciel>] , un logiciel est l'ensemble des éléments informatiques qui permettent d'assurer une tâche ou une fonction.

Exemple : logiciel de comptabilité, logiciel de gestion des prêts.

Le terme a été inventé en 1967 pour remplacer le terme anglais "*software*".

Le logiciel[On utilise aussi le terme de programme ou d'application.] est la partie non tangible de l'ordinateur. Le logiciel qui permet aux autres logiciels de fonctionner et qui gère aussi les ressources matérielles de la machine (écran, clavier, ...) sur un ordinateur donné s'appelle *système d'exploitation*.

Pour créer un logiciel, la manière la plus courante est de l'écrire dans un langage informatique compréhensible par des humains, et ensuite de le traduire en code binaire. Cette traduction est effectuée par un logiciel appelé *compilateur*. Le code binaire est incompréhensible pour l'homme.

Le logiciel dans sa forme compréhensible est appelé source du logiciel, ou source du programme (parfois aussi "*code source* "), et dans sa version en langage machine, il est appelé "*binaire*" (ou exécutable).

Une analogie



Analogie

Imaginons que vous vous trouvez dans un restaurant et que vous mangez un excellent plat. Peut-être aurez-vous l'envie de pouvoir le cuisiner chez vous pour vos amis ?

En informatique, il en va de même pour un logiciel. Le code source est la recette, le binaire est le plat déjà cuisiné.

La plupart des logiciels dits logiciels propriétaires sont distribués sans leur code source et il est interdit d'essayer de comprendre leur fonctionnement, de les partager avec vos amis ou d'essayer de les modifier pour les adapter à vos besoins à la différence des logiciels à code ouvert (*open source*).

Partie A. Les licences des logiciels

Avant de commencer à utiliser des logiciels, on vous demande le plus souvent d'accepter sa licence. La plupart du temps, cela se passe comme avec les contrats d'assurance, on accepte sans avoir lu. C'est pourtant un document bien intéressant.

1. Le contenu des licences

Voici le contenu typique d'une licence de logiciel :

- ◆ Garantie ;
- ◆ Droit d'utilisation ;
- ◆ Droit de copie ;
- ◆ Droit de modification ;
- ◆ Clauses particulières.



Aucune garantie

Toutes ces licences se caractérisent par *une clause de non responsabilité*. Cette clause se situe généralement en fin de licence et est souvent notée en majuscule. Quelle que soit la licence, l'éditeur ne peut être tenu responsable de tout dysfonctionnement dû à l'utilisation du logiciel. L'utilisation de logiciels s'effectue donc à vos risques et périls.



Remarque : Clauses particulières

Vous pouvez y trouver par exemple :

- ◆ le droit à l'utilisation d'une ou plusieurs langues ;
- ◆ la limitation du nombre de processeurs sur un même ordinateurs par lequel le logiciel peut être utilisé ;
- ◆ la limitation du nombre de connexions distantes ;
- ◆ le droit du producteur du logiciel de télécharger automatiquement sur votre machine les mises à jour ;
- ◆ etc.

2. Les types de licence

Vous entendez les termes logiciel libre, freeware, shareware, logiciel du domaine public, ...

Comment les comprendre ?

Voici quelques exemples de ces formes de distribution qu'il ne faut pas confondre avec le logiciel libre défini plus loin :

◆ **Freeware**

Un "*freeware*", contrairement au "*free software (ou logiciel libre en français, terme qui sera longuement expliqué plus loin)*", indique simplement que le logiciel fourni est gratuit, indépendamment de sa licence d'utilisation. Dans certains cas, ce sont des logiciels du domaine public. Le code source du programme n'est pas disponible, ce qui interdit, par exemple de corriger des bogues ou d'effectuer des améliorations.

◆ **Shareware**

Un "*shareware*" est un logiciel dont l'auteur demande aux utilisateurs réguliers de son programme une rétribution volontaire. La rediffusion ou la modification d'un tel programme n'est pas autorisée.

◆ **Logiciel du domaine public**

Un *logiciel du domaine public* n'est plus soumis au droit d'auteur. Si le code source est dans le domaine public, c'est un logiciel libre, mais très souvent le code source n'est pas disponible (seul le code binaire est disponible). Dans ce cas, ce n'est pas un logiciel libre.

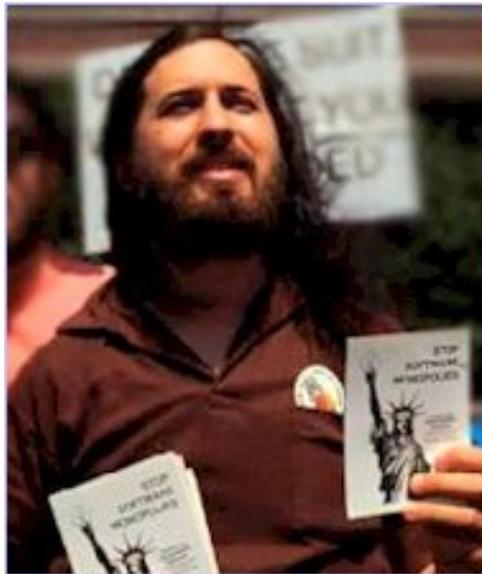
Parfois, on utilise le terme "*domaine public*" d'une façon peu précise pour dire "*libre*" ou "*disponible gratuitement*". Toutefois, "*domaine public*" est un terme légal qui signifie précisément que le logiciel n'est pas "*soumis au droit d'auteur*".

Partie B. Les logiciels libres

Exercice n°1. Que savez-vous des logiciels libres ?

Notez ce que vous savez ou ce que vous avez entendu dire sur les logiciels libres. A la fin de ce chapitre, vous comparerez vos idées du départ à ce que vous aurez appris ...

1. Historique : Au début, il y avait Stallman...



▲ IMG. 1 : RICHARD STALLMAN - SPÉCIFIQUE

Celui qui vous voyez ci-dessus, *Richard Matthew Stallman*, est le fondateur de l'idée du logiciel libre. Il travaille au département de recherche en intelligence artificielle du MIT quand il annonce, en 1983, le *développement d'un système d'exploitation libre* qu'il nomme *GNU*.

L'acronyme récursif GNU signifie *GNU is Not Unix* (« *GNU n'est pas UNIX* »). Le système d'exploitation GNU vise à être un équivalent libre d'Unix. Peu après, il crée la *Free Software Foundation (FSF)*, un organisme sans but lucratif qui permettra l'embauche de programmeurs et la mise sur pied d'une infrastructure légale pour la communauté du logiciel libre.



▲ IMG. 2 : DESSIN DE FSF DU GNU - SPÉCIFIQUE

Afin de s'assurer que tous les logiciels libres développés pour le système d'exploitation GNU restent libres, Richard Stallman popularise le concept de *copyleft*, une utilisation du droit d'auteur permettant d'assurer la protection légale des quatre libertés fondamentales des utilisateurs d'ordinateurs.

En 1989, la première version de la licence publique générale GNU est publiée. Cette licence sera utilisée pour protéger la majeure partie du système GNU qui est alors très avancé, mais encore incomplet. En effet, il manquait le noyau de système d'exploitation. Celui-ci sera créé en 1991 par Linus Torvald sous le nom de *Linux*.

Stallman lance encore en 1999 dans *The Free Universal Encyclopedia and Learning Resource*, l'idée à la base de l'encyclopédie libre *Wikipédia*. Depuis quelques années, il fait campagne contre les brevets logiciels et la gestion des droits numériques (DRM).



Chanson de Stallman

◆ Chanson de Stallman à découvrir à l'adresse suivante :

- <http://framablog.org/index.php/post/2007/01/14/Stalman-Guantanamera> [<http://framablog.org/ind>

2. Les 4 libertés du logiciel libre

Comment peut-on définir le logiciel libre ?

Écoutons donc une des personnes les mieux placées en France : Frédéric Couchet de l'association APRIL [Association pour la Promotion et la Recherche en Informatique Libre].

- ◆ Vidéo APRIL "Qu'est-ce qu'un logiciel libre ?" à visionner à l'adresse suivante :

- <http://framablog.org/index.php/post/2006/09/30/Logiciel-libre-definition> [<http://framablog.org>]

Exercice d'application

Reprenez maintenant les informations concernant les logiciels libres que vous avez notées au début de l'étude de ce chapitre et comparez les aux 4 libertés du logiciel libre qu'on peut résumer ainsi :

- ◆ Liberté d'exécution, sans restriction de temps, de lieu, de motif, de personne, etc. ;
- ◆ Liberté d'étudier le fonctionnement du programme et de l'adapter à ses besoins ;
- ◆ Liberté de redistribuer des copies ;
- ◆ Liberté d'améliorer et de diffuser les améliorations.

Vous avez compris toute la signification de la différence entre les *logiciels propriétaires* « fermés » et les *logiciels libres propices à l'ouverture*.

3. Coût du logiciel libre

Notons que le terme logiciel libre vient de l'anglais *Free Software* où *free* s'entend dans le sens de *free speech* (*libre expression*) et non pas *free beer* (*gratuité*).



Attention

Logiciel libre ne signifie pas "*non-commercial*" ou *gratuit* !

Un logiciel libre doit être disponible pour un usage commercial, pour le développement commercial et la distribution commerciale. Le développement commercial de logiciel libre n'est plus l'exception; de tels logiciels libres commerciaux sont très importants.

Le logiciel libre s'oppose au logiciel propriétaire qui n'offre pas les "quatre libertés" citées antérieurement.

"*Commercial*" et "*propriétaire*" ne sont donc pas synonymes : si la plupart des logiciels commerciaux sont propriétaires, il en existe aussi des libres ; il existe de même des logiciels non-commerciaux libres et d'autres non-libres.

4. Galerie non-exhaustive de logiciels libres

Dorénavant, il existe presque dans chaque domaine, à côté des logiciels propriétaires des variantes libres plus ou moins abouties.

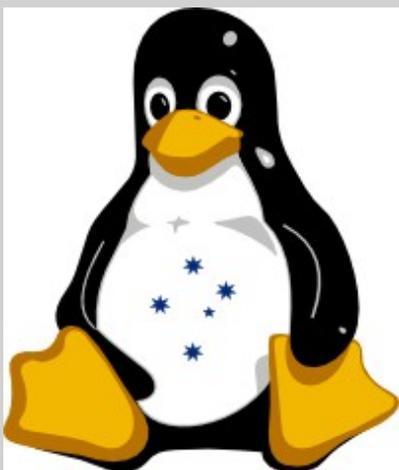
Nous montrons donc ci-dessous quelques logos et caractéristiques des logiciels libres les plus répandus (loin de toute exhaustivité, bien sûr).



GNU, le système d'exploitation lancé par Stallman en 1984, est l'ancêtre de tous les autres logiciels libres.

◆ Site Web :

- <http://www.gnu.org/home.fr.html> [<http://www.gnu.org/home.fr.html>]



Le pingouin *Tux* est la mascotte de *Linux* - noyau du système d'exploitation libre initié par Linus Torvald en 1991.

Il s'agit de la couche de bas niveau qui s'occupe de fournir aux logiciels une interface pour communiquer entre eux et avec le matériel. Tux est devenu le symbole du logiciel libre en général.

◆ Site Web :

- <http://www.linux-france.org/> [<http://www.linux-france.org/>]



Suse est une de nombreuses *distributions Linux* (les autres, étant *Ubuntu, Debian, RedHat, Mandriva, etc.*).

Les distributions (particularité du système d'exploitation Linux) rassemblent les composants d'un système GNU/Linux dans un ensemble cohérent et stable facilitant son installation, utilisation et maintenance. Elles comprennent donc le plus souvent un logiciel d'installation et des outils de configuration.

◆ Site Web :

- <http://www.framasoft.net/article2334.html> [<http://www.framasoft.net/article2334.html>]



Firefox est un navigateur Web développé et distribué par la *Fondation Mozilla* aidée de *centaines de bénévoles* grâce aux méthodes de développement open source.

Le nom *Firefox* (à ne pas confondre avec fire fox qui signifierait « renard de feu » en anglais) est le nom anglais du « *panda rouge* » qui est la mascotte du projet. Ce logiciel est sorti en octobre 2005 et le nombre de téléchargements a dépassé 200 millions, en été 2006.

◆ Site Web :

- <http://www.firefox.fr/> [<http://www.firefox.fr/>]

Thunderbird (qu'on pourrait traduire comme "oiseau d'orage") est un *outil de messagerie complet*.



Thunderbird supporte les protocoles *IMAP* et *POP* (vous comprendrez ces termes en étudiant le B6) ainsi que le formatage des messages en *HTML*. Sa gestion intégrée des fils d'actualités (*RSS*) (voir le B7), ses puissantes fonctions de recherche et sa gestion très avancée du filtrage en font un outil particulièrement performant.

◆ Site Web :

- <http://www.mozilla-europe.org/fr/products/thunderbird/> [<http://www.mozilla-europe.org>]



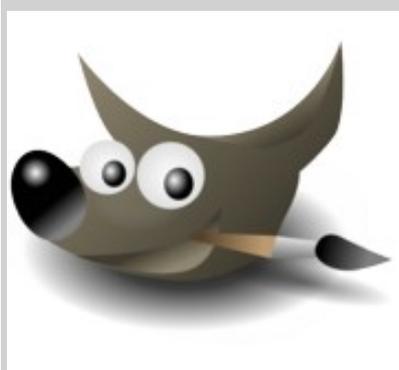
OpenOffice est une suite bureautique complète. En sa version actuelle, elle atteint une maturité telle qu'elle ne souffre plus de quelconques comparaisons avec ses homologues propriétaires. Elle est composée :

- ◆ d'un traitement de texte : *Writer* ;
- ◆ d'un tableur : *Calc* ;
- ◆ d'un logiciel de présentation : *Impress* ;
- ◆ d'un logiciel de dessin vectoriel : *Draw* ;
- ◆ d'un éditeur de pages web ;
- ◆ d'un module de création et de gestion des bases de données : *Base*.

Elle est compatible en lecture et en écriture (et donc en modification) avec les fichiers issus de la suite bureautique Microsoft Office version XP (et des versions antérieures 2000, 97 etc...) ainsi qu'avec les fichiers WordPerfect.

◆ Site Web :

- <http://fr.openoffice.org/> [<http://fr.openoffice.org/>]



GIMP - acronyme de *GNU Image Manipulation Program* - est un logiciel de traitement d'image. *GIMP* occupe une place particulière dans l'informatique libre : il est considéré comme le premier des logiciels libres à la fois grand public et de qualité professionnelle. Sa disponibilité a incité un certain nombre d'utilisateurs à installer une distribution Linux pour la première fois.

La mascotte officielle de *GIMP* (fabriquée avec *GIMP*, bien sûr) s'appelle Wilber.

◆ Site Web :

- <http://www.gimp-fr.org/news.php> [<http://www.gimp-fr.org/news.php>]



Ogg Vorbis est une technologie d'encodage et de streaming audio professionnelle, complètement ouverte et sans brevet, avec tous les avantages de l'Open Source. Le format fermé et privé .mp3 n'a qu'à bien se tenir car le format ouvert .ogg est libre, multi-plateforme, supporté par la plupart des players et au rendu excellent.

◆ Site Web :

- <http://www.vorbis.com/> [<http://www.vorbis.com/>]

▲ TAB. 1 : LISTE DE LOGICILES LIBRES

B. Connaître les règles de création et d'échange

L'état français se préoccupe de l'interopérabilité numérique pour garantir l'efficacité et la sécurité des échanges électroniques. Un de derniers documents synthétiques publiés concernant ce sujet, le *Référentiel Général d'interopérabilité (RGI)*, recommande chaque fois que c'est possible des formats ouverts et déconseille les formats propriétaires.

Ce document, facile à manipuler, peut vous être très utile .

◆ Cliquez [ici](http://www.ateliers.modernisation.gouv.fr/ministeres/domaines_d_expertise/archite) pour ouvrir le document. [[http://www.ateliers.modernisation.gouv.fr/ministeres/domaines d expertise/archite](http://www.ateliers.modernisation.gouv.fr/ministeres/domaines_d_expertise/archite)]

Dans la suite de ce didacticiel, nous avons pris le soin de vous présenter chaque fois que c'était possible les logiciels libres à côté des variantes propriétaires : Writer ET Word, Calc ET Excel, etc.



Remarque

N'oubliez pas que les documents créés avec les logiciels libres sont lisibles par des programmes propriétaires ainsi que par des programmes à code ouvert mais l'inverse n'est pas vrai !

C. Quelques ressources consultée lors de la rédaction de ce chapitre

Voilà les ressources sur lesquelles nous nous sommes basés pour rédiger ce chapitre. Vous pouvez aller les voir si vous souhaitez approfondir telle ou telle notion abordée de manière rapide ci-dessus :

◆ **Futura Sciences - Au coeur de la science**

<http://www.futura-sciences.com/> [<http://www.futura-sciences.com/>]

◆ **Wikipédia**

<http://fr.wikipedia.org/wiki/Accueil> [<http://fr.wikipedia.org/wiki/Accueil>]

◆ **Dicofr.com - Dictionnaire de l'informatique et d'Internet**

<http://www.dicofr.com/> [<http://www.dicofr.com/>]

◆ **Tout-Savoir.net**

<http://www.tout-savoir.net/> [<http://www.tout-savoir.net/>]

◆ **Techno-Science.net**

<http://www.techno-science.net/> [<http://www.techno-science.net/>]

◆ **Framasoft**

<http://www.framasoft.net/> [<http://www.framasoft.net/>]

◆ **Association pour la Promotion et la Recherche en Informatique Libre - APRIL**

<http://www.april.org> [<http://www.april.org>]

◆ **Association des Développeurs et des Utilisateurs de Logiciels Libres pour l'Administration et les Collectivités Territoriales - ADULLACT**

<http://www.adullact.org/> [<http://www.adullact.org/>]

Synthèse

Dans ce chapitre, vous avez appris :

- ◆ ce qu'est un logiciel,
- ◆ quelles sont les différentes licences s'appliquant à des logiciels,
- ◆ ce qu'est un logiciel libre : son historique, ses caractéristiques mais surtout les applications du monde libre qui vous seront immédiatement utiles.

Testez-les, vous avez appris dans ce chapitre que vous pouvez les télécharger en toute légalité et les essayer.

Si vous avez besoin d'accompagnement pour les utiliser, notre didacticiel sera votre compagnon !

La tour de Babel des systèmes d'exploitation, des normes et des standards

Préambule

Quand vous achetez un logiciel il vous faut être sûr qu'il va fonctionner sur votre ordinateur.

Et quand vous réalisez un document pour l'envoyer à votre voisin, il faut être certain que celui-ci pourra l'utiliser.

En fait, chaque ordinateur fonctionne avec un système d'exploitation, dont le principe est décrit dans le *module B1- "S'approprier son environnement de travail"*.

Ce *système d'exploitation* [En anglais, Operating System ou OS.] est un ensemble de programmes responsables de la liaison entre les ressources matérielles d'un ordinateur et les applications de l'utilisateur [Traitement de texte, tableur, jeu vidéo, etc.]. Il assure le démarrage de l'ordinateur, et fournit aux applications logicielles de l'ordinateur une liaison générique avec les périphériques matériels de cet ordinateur [Le périphérique permet de faire communiquer ensemble par exemple : le logiciel pour lire de la musique et la carte son et les enceintes.].

Il existe différents systèmes d'exploitation ainsi ... :

- ◆ La société *Microsoft* a créé successivement *Microsoft Dos*, puis *Microsoft Windows*, les deux dernières versions de *Microsoft Windows* étant *Windows XP* et maintenant *Windows Vista*. Ces systèmes d'exploitations sont actuellement de loin les plus utilisés par les particuliers et correspondant au plus grand parc possible de logiciels et de matériels informatiques différents.
- ◆ La société *Apple* propose des systèmes d'exploitation *Mac OS* réputés pour leur simplicité d'utilisation, la dernière version s'appellant *Mac OS X* (et représentant environ 5% des utilisateurs d'ordinateurs personnels).
- ◆ Et le monde du logiciel libre a créé le système d'exploitation *Linux* avec une multiple descendance (distributions *Red Hat*, *Mandriva*, *Unbutu*, *Debian*,...) qui a une diffusion limitée auprès du grand public et très étendue par contre pour l'administration serveur et web, puisque près de 40% des OS utilisés dans ces domaines d'application sont des OS *linux/Unix*.

Il existe de grandes querelles autour des comparaisons entre les différents systèmes d'exploitation, chaque tenant d'un système (*Windows*, *Mac* ou *Linux/Unix*, soutenant que son système est comparativement meilleur que les autres).

Nous ne rentrerons pas dans cette controverse, on notera néanmoins que l'existence de différents systèmes d'exploitation rend obligatoire l'existence de normes pour pouvoir communiquer entre systèmes. D'autant plus qu'il existe une seconde couche d'application, après ces systèmes d'exploitation, constitués par les logiciels que l'utilisateur va installer sur son ordinateur.

Ainsi chacun va installer un *navigateur web* (*Firefox*, *Internet Explorer*, ...), une suite bureautique (*Open Office*, *Microsoft Office*, ...), un logiciel pour lire de la musique (*Win Amp*, *Windows Media Player*, ...), un logiciel pour communiquer avec d'autres personnes (*Skype*, *Msn*, ...), un gestionnaire de mails, des logiciels professionnels correspondant à votre domaine d'activité (*Autocad* si vous travaillez dans le secteur des *BTP* par exemple ou un logiciel de comptabilité si vous exercez dans ce domaine), et enfin des logiciels correspondant à vos centres d'intérêts privés (exemple généalogie, jeux, cuisine, etc.)

Questions

- ◆ Mais comment être certain que mon logiciel de communication va communiquer avec celui de mon correspondant sur Internet ?
- ◆ Comment savoir si mon arbre généalogique que j'ai mis 6 mois à réaliser sur mon logiciel adéquat pourra être exporté sur le nouveau logiciel de généalogie que je viens d'acquérir ?
- ◆ Comment avoir la certitude que ce CV que j'ai envoyé à cette petite société d'agro-alimentaire sera bien lu par le logiciel de traitement de texte qu'utilise le responsable du recrutement de cette entreprise ?

Les problèmes auxquels l'utilisateur de tous ces programmes sera vite confronté resteront des problèmes de compatibilité et d'interopérabilité ce qui débouche sur la notion de norme et de standard.

Définitions

Nous avons retenu les définitions et articles proposées sur Wikipédia [<http://fr.wikipedia.org/wiki/Accueil>] .



Compatibilité

On entend par *compatibilité* la capacité de deux systèmes à communiquer sans ambiguïté.



Interopérabilité

L'*interopérabilité*, c'est la capacité à rendre compatibles deux systèmes quelconques. L'*interopérabilité* nécessite que les informations nécessaires à sa mise en œuvre soient disponibles sous la forme de standards ouverts.

A. L'interopérabilité

L'interopérabilité est une notion absolument cruciale pour le réseau téléphonique mondial et Internet.

Par essence, des matériels divers et variés sont mis en œuvre dans ces réseaux hétérogènes aux côtés d'une panoplie encore plus vaste de matériels informatiques et de logiciels.

Elle est aussi cruciale pour l'ensemble de l'économie, car dans presque tous les domaines d'activité dans l'industrie, dans les services, et même en agriculture, on emploie des systèmes informatiques, qui aujourd'hui communiquent d'une entreprise à l'autre par l'intermédiaire de réseaux informatiques (Internet, extranet, messageries électroniques).

L'interopérabilité nécessite que les communications obéissent à des normes, clairement établies et univoques (voir Normes et standards industriels).

Ces documents techniques définissent souvent des exigences, parfois accompagnées de recommandations plus ou moins optionnelles. Si la norme est correctement écrite, deux systèmes qui satisfont aux exigences doivent dialoguer ensemble sans souci particulier.

Ils peuvent ainsi évoluer librement sans risque de casser cette possibilité de communication, tant qu'ils respectent la norme définissant leurs interfaces.



Exemple

La norme peut définir des éléments comme :

- ◆ les formats des données échangées dans le contexte considéré, qui décrivent des séquences d'informations ou de commandes qu'un système doit envoyer, comment ses correspondants doivent y répondre (protocole de communication) ;
- ◆ les tensions et courants à utiliser ;
- ◆ les types de câbles à utiliser.



Distinction entre norme et standard

Dans le monde de l'informatique en particulier, il ne faut pas faire la confusion entre une norme et un standard, ce dernier désignant ce qui est produit habituellement par un producteur et ne dépend que de lui. Cette confusion vient de l'anglais, qui n'a qu'un seul mot pour désigner les deux concepts, standard signifiant aussi norme.



Remarque

Il existe deux approches de l'interopérabilité celle des *normes ouvertes* et celle des *formats propriétaires*.

Quelles questions pour quel format ?

Pour un questionnement professionnel avant l'acquisition d'un logiciel, sur le blog "[Format ouvert \[http://formats-ouverts.org/\]](http://formats-ouverts.org/) ", on propose de réfléchir à 5 domaines spécifiques préalables :

1. Technique

Et les formats ? Les formats de fichiers, les protocoles ou les langages de programmation utilisés sont-ils ouverts ?

2. Information

Et les métadonnées ? Les informations sur les informations (auteur, titre, date,...) sont-elles ouvertes ?

3. Juridique

Et la licence ? Qu'en est-il précisément des droits d'utilisation des informations, des logiciels ou des technologies ?

4. Matériel

Et les supports ? Les matériels (ordinateurs, assistants personnels) et les supports (CD, disques durs,...) avec leurs prises (USB, Firewire,...) sont-ils toujours disponibles ?

5. Administratif

Et la gestion ? Un suivi précis de la vie des documents et des supports est-il en place ?

Les réponses à ces questions sont capitales pour l'interopérabilité et l'archivage, mais aussi pour l'innovation, la sécurité, la concurrence et l'indépendance de la structure qui effectue des choix logiciels.

B. Les normes ouvertes et communautaires

Ce sont des normes, dont les caractéristiques sont publiées, qui peuvent être utilisées par tous et mises en place librement par tout développeur.

Généralement, ces normes ouvertes sont élaborées et maintenues par des organismes officiels et (ou) des communautés de gens intéressés, comme la communauté Free Software Open Source.



Exemples de normes ouvertes

- ◆ XML ;
- ◆ XHTML (Web) ;
- ◆ PNG (Image) ;
- ◆ Ogg Vorbis (Son) ;
- ◆ etc.

C. Les formats fermés et propriétaires

À l'opposé, le frein majeur à une interopérabilité optimale est l'utilisation dans des matériels et logiciels de formats dont seuls leurs concepteurs auraient les clefs.

Cette fermeture est souvent volontaire car elle vise, dans le cas d'un format de fichier propriétaire, à s'assurer qu'un utilisateur n'utilisera pas un autre logiciel pour lire ses données.

De plus, le fait de ne pas publier officiellement ces formats permet à la société de pouvoir modifier son format de fichier lorsqu'elle change de version de son logiciel, sans avoir de compte à rendre à personne. Même si certains développeurs arrivent, à force de tâtonnements, à écrire des logiciels en utilisant ces formats, rien ne les préserve d'une modification de ces derniers rendant leurs logiciels incompatibles.



Exemple

Les messageries instantanées propriétaires comme ICQ, Yahoo! Messenger ou MSN Messenger dont les protocoles ne sont pas compatibles et maintenus non-interopérables.

D. Entre les deux : les normes à distribution restreinte

Entre ces deux mondes, il existe également un grand nombre d'organismes plus ou moins ouverts dans la sélection de leurs membres, souvent orientés vers les entreprises et ayant des cotisations ou des droits d'entrées conséquents, dont les publications ne sont pas librement accessibles, mais payantes. C'est le cas de la majorité des organismes d'État, notamment. On peut citer les organismes ISO, ANSI, AFNOR, UIT...

Parfois, c'est une très petite assemblée de personnes, voire une seule, qui décide d'une norme. Elle peut être plus ou moins à l'écoute des suggestions, bien sûr, de ses utilisateurs. Des exemples courants sont *RAR* (algorithme de compression), *PDF* (format de document pour l'impression), *Java* (langage de programmation), *Flash* (format d'animation pour le Web), etc.

E. Relation entre l'informatique et l'interopérabilité

L'informatique pose le problème de l'*interopérabilité* en des termes nouveaux. Elle met en évidence certaines contradictions entre les intérêts commerciaux d'entreprises fournissant produits et services, et les exigences nouvelles des consommateurs de ces produits et services.

Du fait des outils informatisés, de l'expertise acquises par des groupes d'utilisateurs, de la communication facilitée, l'interopérabilité devient une problématique plus concrète aux yeux d'un nombre grandissants de personnes, qui en comprennent mieux les tenants et aboutissants - notamment les enjeux du choix et de la protection des données.

Ce mouvement est vu comme une avancée démocratique par les partisans d'une *interopérabilité* « ouverte », mais cet avis n'est pas partagé par tous. Nombre d'entreprises défendent à l'inverse un modèle plus classique où l'interopérabilité reste le fruit de l'initiative privée et subit un contrôle strict. De par les enjeux qui lui sont aujourd'hui liés, dans les domaines du travail ou dans la sphère privée par exemple, l'interopérabilité informatique va certainement jouer un rôle de catalyseur des changements futurs, quels qu'ils soient.

F. Interopérabilité en bureautique

Pendant longtemps, chaque éditeur de logiciel fabriquait son logiciel, et des filtres pour faire migrer les clients utilisateurs de leur suite bureautique à la nouvelle. L'échange de document n'était pas garanti.

Depuis peu, sous l'impulsion d'*OpenOffice.org* [Soutenu par Sun Microsystems.], deux systèmes d'échange de fichier bureautique ont été créés, dont l'un d'entre eux est l'*OpenDocument*. L'autre étant celui de *Microsoft*.

Cependant, en 2006, en France, dans le secteur privé bon nombre de documents continuent à circuler au format *.doc* de *Microsoft Word*, cette utilisation du format *Word* pose un problème d'interopérabilité, dans la mesure où :

- ◆ soit le destinataire doit acheter la bonne version de *Microsoft Word* (et éventuellement une version de *Windows*) pour lire de tels documents ;
- ◆ soit, en utilisant *OpenOffice.org*, il existe un risque que certaines parties du document, utilisant des fonctionnalités non connues d'*OpenOffice* ne passent pas correctement ou soient déformées.

On le voit, la notion de standard en informatique est avant tout pragmatique. On est bien loin de la notion de "norme". Pour s'en convaincre, il suffit de s'arrêter sur les formats de document de *Microsoft Office*. Ces formats (qu'il s'agisse de *Word*, d'*Excel*, de *Powerpoint*, etc.) ne sont évidemment pas des standards de droits. En revanche, ce sont des standards de fait, à tel point que des outils concurrents (comme *OpenOffice*, suite bureautique dont le code source est ouvert) affichent parmi leurs qualités premières leur aptitude à gérer ces formats..



Remarque : Recommandation de la commission européenne

Dans sa *recommandation n°2*, la Commission européenne donne la priorité à l'utilisation de standards ouverts. Par standard ouvert, elle entend :

- ◆ Le standard a été adopté et sa maintenance sera assurée par une organisation sans but lucratif, et son développement ultérieur se fera sur la base d'une procédure décisionnelle ouverte accessible à toutes les parties intéressées (consensus ou décision majoritaire, etc.).
- ◆ Le standard a été publié et le document de spécification du standard est disponible soit gratuitement soit contre une somme symbolique. Tout le monde doit pouvoir copier, distribuer et utiliser ce document gratuitement ou contre une somme symbolique.
- ◆ Les droits de propriété intellectuelle, à savoir les brevets éventuels, du standard (ou de parties du standard) sont irrévocablement mis à disposition sans exiger de redevance.



Organismes majeurs publiant des normes

Il existe différents organismes dont le rôle est de valider des normes que les industries, notamment, utiliseront comme support pour rendre leurs services et produits interopérables, et a fortiori, compatibles.

- ◆ **ISO**
Organisation internationale de normalisation
- ◆ **ANSI**
American National Standards Institute
- ◆ **AFNOR**
Association française de normalisation
- ◆ **CEN**
Comité européen de normalisation
- ◆ **ITU**
Union internationale des télécommunications
- ◆ **CENELEC**
Comité européen de normalisation électrotechnique

Pour l'Internet en particulier :

- ◆ **IETF**
Internet Engineering Task Force
- ◆ **ISOC**
Internet Society
- ◆ **W3C**
World Wide Web Consortium
- ◆ **OASIS**
Organization for the Advancement of Structured Information Standards

Les formats de fichiers ouverts pour l'échange de l'information

A l'instar de la commission Européenne, le gouvernement français, par l'intermédiaire de la Direction Générale de la Modernisation de l'Etat du ministère du budget et de la réforme de l'Etat, prépare un Référentiel Général d'Interopérabilité [http://www.ateliers.modernisation.gouv.fr/ministeres/domaines_d_expertise/arc], qui fait suite au Cadre Commun d'interopérabilité élaboré et publié en septembre 2003.

Le *Référentiel Général d'Interopérabilité (RGI)* guidera l'administration dans ses choix pour les évolutions de son environnement numérique. Dans ce référentiel, on trouve une partie technique précisant les formats à utiliser pour chaque type de ressources. Ces préconisations sont soit *obligatoires* soit des *recommandations fortes* mais, dans les deux cas, elles sont de bon conseil pour le particulier car elles risquent de devenir la référence dans l'échange de données informatisées.

Ce chapitre vous présente les recommandations les plus importantes concernant les formats de fichiers à utiliser.

A. Formats des images fixes et des animations

Le tableau ci-dessus vous présente les formats de fichiers obligatoires, recommandés ou interdits par le RGI selon l'usage prévu de la ressource, qu'il s'agisse d'une illustration photographique ou non, d'images qui ne doivent pas être compressées, d'images TIFF, d'animations graphiques simples ou complexes.

	<i>Obligatoire</i>	<i>Recommandé</i>	<i>Interdit</i>
Echanges d'illustrations non photographiques (par exemple : schéma, icône ou logo)	PNG	-	-
Présentation (affichage) d'illustrations non photographiques	-	-	GIF
Echange et présentation d'illustrations photographiques	JPG	-	-
Echanges d'images qui ne doivent pas être compressées.	TIFF	-	-
Présentation d'images TIFF	TIFF	-	-
Animations graphiques simples et/ou de courte durée	-	GIF	-
Animations graphiques complexes et/ou de plus longue durée	-	Flash	-

▲ TAB. 2 : FORMATS DES IMAGES FIXES ET DES ANIMATIONS

▲ IMG. 11



Attention

Il est DÉCONSEILLÉ d'utiliser les formats *EPS*, *PICT*, *BMP*, *PCX* pour l'échange et la présentation d'images.



Format PNG

PNG (Portable Network Graphics) est un format de fichier graphique de type Bitmap (non-vectoriel). Il a été conçu par une communauté de développeurs afin de fournir un format ouvert, alternatif au format GIF pour la compression sans pertes. Ce format est promu par l'association W3C et par l'ISO.



Norme JPEG

La *norme JPEG (Joint Photographic Experts Group)*, définie par l'ISO, est très utilisée pour la photographie numérique. Elle permet un haut niveau de compression qui convient particulièrement à la compression de photographies. Le taux de compression est réglable. La contrepartie de ce taux de compression est une perte d'information. JPEG fonctionne en mode RVB 24 bits et permet donc une excellente reproduction de couleurs demi teintes.



Format GIF

GIF (Graphic Interchange Format) est un format très répandu mis au point par la société CompuServe en 1987. Ce format étant propriétaire (Unisys), il y a lieu de veiller à migrer dès que possible les fichiers GIF en fichiers PNG. GIF fonctionne uniquement en mode 8 bits, 256 couleurs indexées au maximum. Il utilise une méthode de compression sans perte, donc réversible.



GIF animé

Le *GIF animé* est un format répandu. En 1989, le format GIF pour image fixe a été étendu pour permettre le stockage de plusieurs images dans un même fichier et pour définir leur séquençement. Ceci permet de créer des diaporamas, voire des animations simples (bandeau par exemple) si les images sont affichées à un rythme suffisamment soutenu. Par ailleurs, chaque image d'une animation peut avoir sa propre palette de couleurs.



Flash

Flash est un format répandu qui permet de réaliser des animations graphiques complexes ainsi que de longue durée. C'est un format propriétaire développé par la société Macromedia. Cette société a été rachetée par la société Adobe Systems en décembre 2005.

➤ Voir Fiche-Complément en fin de fascicule :

"Qu'est-ce qu'une image numérique ?"

➤ Voir Fiche-Complément en fin de fascicule :

"Les différents types de palettes"

B. Formats pour le son et la vidéo

Le tableau ci-dessus vous présente les formats de fichiers obligatoires, recommandés, déconseillés ou interdits par le RGI selon l'usage prévu de la ressource, qu'il s'agisse d'une séquence sonore, d'une séquence vidéo Basse ou Haute Définition

	<i>Obligatoire</i>	<i>Recommandé</i>	<i>Déconseillé</i>	<i>Interdit</i>
Diffuser et sauvegarder des séquences sonores	-	MP3	WAV, WMA	-
Présentation de séquences vidéo basse définition	MPEG-2	-	-	-
Echanges de séquences vidéo basse définition	-	-	-	-
Présentation de séquences vidéo Haute Définition	-	MPEG-4	-	-
Echanges de séquences vidéo Haute Définition	MPEG-4	-	-	-

▲ TAB. 3 : FORMATS POUR LE SON ET LA VIDÉO

▲ IMG. 12



Format MP3

MP3 est l'abréviation de *MPEG-1/2 Audio Layer 3*, la spécification sonore du standard MPEG-1, du Moving Picture Experts Group (MPEG).

C'est un algorithme de compression capable de réduire fortement la quantité de données nécessaire pour restituer du son stéréophonique. Pour l'auditeur, le son reproduit ressemble à une reproduction du son original non compressé, c'est-à-dire avec perte significative mais de qualité sonore acceptable pour l'oreille humaine.

Bien que le MP3 soit souvent perçu par l'utilisateur final comme une technologie gratuite, cette technologie fait l'objet d'une licence car elle intègre des algorithmes brevetés. L'algorithme « MPEG-1 Layer 3 » décrit dans les normes ISO est soumis à des royalties à Fraunhofer IIS et Thomson (les

détenteurs du brevet) pour toute utilisation commerciale ou implémentation physique (notamment sur les baladeurs MP3).



Format WAV (RIFF WAVE)

À l'origine, format de fichier sonore de Microsoft Windows, il est maintenant élargi à d'autres plates-formes. Par rapport au format MP3, il a l'inconvénient d'être beaucoup plus volumineux.



Format WMA

Le format *WMA* offre pour spécificité la possibilité de protéger dès l'encodage les fichiers de sortie contre la copie illégale par une technique nommée *DRM* (*Digital Right Management*) que l'on traduit en français par *GDN* (*Gestion des Droits Numériques*).

Il est à noter qu'il n'existe pas de standard sur cette technique.



Ogg Vorbis

Ogg Vorbis est un algorithme de compression et de décompression (codec) audio numérique, sans brevet, ouvert et libre, avec pertes de données, plus performant en terme de qualité et taux de compression que le format MP3.

Promu par la fondation Xiph.org, c'est un des composants de leur projet Ogg, qui a pour but de créer un ensemble de formats et codecs ouverts multimédia (son, vidéo), libre de tout brevet.

Radio France expérimente le format Ogg Vorbis en diffusant sur Internet, huit de ses principales stations.



Norme MPEG-2

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* 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. Elle intègre cependant des algorithmes brevetés. Ce format vidéo est utilisé pour les DVD, CVD et SVCD avec différentes résolutions d'image. Ce format est également utilisé dans la diffusion de télévision numérique par satellite, câble, réseau de télécommunications ou hertzien (Télévision Numérique Terrestre).

C. Formats pour les documents non structurés et semi-structurés (traitement de texte, tableur, présentation)

Le tableau ci-dessus vous présente les formats de fichiers obligatoires, recommandés ou interdits par le RGI selon l'usage prévu du document semi- ou non-structuré.

	<i>Obligatoire</i>	<i>Recommandé</i>	<i>Interdit</i>
Présentation en ligne de documents non structurés	-	HTML	-
Echanges de documents non structurés	-	-	HTML
Echanges de documents bureautiques semi-structurés (traitement de texte, tableur, présentation)	-	Formats Open Document, Formats basés sur XML (.odt, .ods, .odg)	-
Conservation des documents non structurés et semi-structurés	PDF	-	-

▲ TAB. 4 : FORMATS POUR LES DOCUMENTS NON STRUCTURÉS ET SEMI-STRUCTURÉS

▲ IMG. 13



Format HTML

HTML (HyperText Markup Language) est un langage créé et utilisé pour écrire les pages Web. HTML permet en particulier d'insérer des hyperliens dans du texte, donc de créer de l'hypertexte, d'où le nom du langage.



OpenDocument

Open Document (Open Document Format for Office Applications) est un format ouvert basé sur le langage XML pour les documents de type bureautique. Il est basé sur le format créé pour les premières versions de la suite bureautique libre et gratuite [OpenOffice.org](http://fr.openoffice.org/) [http://fr.openoffice.org/], auquel il reste similaire.



Attention

Le RGI précise en outre :

- ◆ *Il est OBLIGATOIRE d'accepter tout document au format Open Document pour les échanges de documents bureautiques semi-structurés (traitement de texte, tableur, présentation).*

ET

- ◆ *Il est INTERDIT de faire une migration depuis le format bureautique couramment utilisé par une organisation, vers un format autre que le format ouvert Open Document.*



Format PDF

Le format *PDF*, ou *Portable Document Format*, est un format propriétaire mis au point par la société Adobe. Il est lié au logiciel Acrobat, et son usage est très répandu.

La spécification PDF/A-1 a été publiée et est utilisée par les organismes de normalisation du monde entier pour garantir la sécurité et la fiabilité de la diffusion et des échanges de documents électroniques. Les sphères publique et privée ont massivement adopté ce format pour simplifier les échanges de document.

Un des principaux avantages de ce format est que les fichiers au format PDF sont 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 le créer.

Adobe diffuse actuellement gratuitement le logiciel de lecture de ce format :

<http://www.adobe.com/fr/products/acrobat/readstep2.html> [<http://www.adobe.com/fr/produ>

D. En pratique

Dans la majorité des cas les échanges d'informations que nous avons à faire avec nos collaborateurs concernent les documents bureautiques, traitement de textes, tableurs, présentations par ordinateur. Le *Référentiel Général d'Interopérabilité* nous recommande fortement l'usage de format *Open Document*, issues de la suite bureautique « OpenOffice [<http://www.openoffice.org>] ».

Pour respecter ces recommandations, La société Microsoft® a écrit un greffon pour sa suite bureautique Microsoft Office® afin que celle-ci puisse utiliser les formats Open Document.

Actuellement, nous sommes dans un monopole de fait du format de Microsoft Office®

, c'est pourquoi la suite bureautique libre et gratuite *OpenOffice* permet la lecture et l'écriture au format Microsoft Office® . Cependant bien que les deux suites soient capables de travailler dans les deux formats, il est fortement recommandé de travailler dans un format *Open Document* car c'est le seul dont les caractéristiques soient officiellement publiées, ce qui assure la réutilisabilité mais aussi la pérennité des ressources produites sous ce format.

Voici quelques exemples de formats de fichiers à préconiser selon les situations. Les choix suivants ne sont pas exclusifs, mais représentent aujourd'hui les choix les plus raisonnables en fonction des actions à réaliser.

Type de fichiers	Action / Contrainte	Format de fichier
Texte, feuille de calcul	Pour la rédaction et la sauvegarde	ODT, ODS (OpenDocument)
	Pour le proposer à la consultation	PDF
	Pour le partager pour collaboration	ODT, ODS, CSV
	Pour le mettre en ligne sur Internet	HTML
Présentation par ordinateur	Pour la création, sauvegarde, partage collaboratif	ODP (OpenDocument)
	Pour la proposer en consultation	PDF
	Pour faire la présentation en ligne	HTML
Photo		JPEG
Graphique	Si moins de 256 couleurs	GIF
Plusieurs fichiers	Pour les envoyer par mail	ZIP
	Pour faire une sauvegarde	ZIP
Vidéo	Pour visionnage local	MPEG4, MPEG2
	Pour la diffuser	MPEG2, MPEG4
Son	Pour écoute, sauvegarde et diffusion	MP3

▲ TAB. 5 : QUEL FORMAT DE FICHIER SELON LA SITUATION ?

▲ IMG. 14



Format ZIP

ZIP est un format de fichier pour la compression de données. La compression de données est utilisée pour réduire la taille des fichiers, facilitant ainsi leur stockage pour sauvegarde mais aussi leur envoi par courrier électronique.

E. Pour en savoir plus

Cadre Commun d'Interopérabilité (CCI)

Vous pouvez télécharger ci-dessous la dernière version du Cadre Commun d'Interopérabilité validé en Septembre 2003. Les formats préconisés pour les données numériques se trouvent de la page 38 à la page 44.

- Voir annexe A en fin de fascicule

Référentiel Général d'Interopérabilité (RGI)

◆ SYNERGIES - Les ressources de l'administration électronique

Espace de mutualisation des acteurs de l'administration électronique.

- Interopérabilité (le RGI) [http://www.synergies-publiques.fr/rubrique.php?id_rubrique=71]

◆ Les ateliers de la modernisation

Les Ateliers de la modernisation, du Ministère du Budget et de la réforme de l'Etat, accueillent des groupes de travail appelés communautés. Ces communautés sont chargées d'élaborer ou de mettre en oeuvre les solutions opérationnelles sur les nombreux sujets liés au thème de la modernisation de l'Etat et des territoires.

Le lien ci-dessous vous permet d'accéder à l'espace relatif au Référentiel Général d'Interopérabilité.

- [https://www.ateliers.modernisation.gouv.fr/ministeres/domaines_d_expertise/architecture fo](https://www.ateliers.modernisation.gouv.fr/ministeres/domaines_d_expertise/architecture)

◆ L'interopérabilité sur le site de la Modernisation de l'Etat

Quelques articles et animations à destination des néophytes pour une sensibilisation à la question de l'interopérabilité.

- <http://www.thematiques.modernisation.gouv.fr/sommaire.php?id=23> [<http://www.thematiques>

Conclusion

Le discours qu'on peut entendre sur les NTIC est souvent manichéen :

- ◆ D'un côté des sociétés et des technophiles nous proposent des mondes meilleurs où tout sera résolu grâce à l'informatique où apprendre deviendra plus facile. Communiquer simultanément et travailler avec efficacité avec différents collaborateurs situés aux quatre extrémités de notre planète deviendra un acte naturel. Chacun maîtrisera simplement tout son équipement informatique. Enfin on nous explique que quoi qu'il arrive, une sorte de train est en marche que rien ne peut arrêter et qu'on doit donc monter dedans que cela nous plaise ou non.
- ◆ De l'autre des technophobes nous parlent de sociétés déshumanisées, de perte de liens sociaux, de fausse révolution et d'effet de mode.

En fait, il faut rétablir certaines vérités et revenir à un langage plus nuancé.

À ce sujet on peut rappeler que malgré de nombreux progrès, l'usage d'un ordinateur est un geste technique compliqué, que les utilisateurs les plus avertis ne sont pas à l'abri de bugs et de problèmes techniques les plus variés. Et que la simplicité décrite de l'utilisation des programmes informatiques demeure souvent une simple utopie.

Pour autant, il faut se rendre compte des transformations incroyables que font surgir l'apparition d'Internet couplée à notre informatique moderne et plus on en maîtrisera la complexité, mieux on pourra influencer sur les usages que nous voulons réaliser avec ces outils.

Fiches-Compléments



Qu'est-ce qu'une image numérique ?

Les images numériques sont constituées d'un ensemble de pixels (picture elements), juxtaposés en lignes et en colonnes. On appelle ces images des *bitmaps*.

Le pixel est le plus petit élément que l'on peut trouver dans une image. Chaque pixel possède des caractéristiques propres : couleur, luminosité, brillance, position. Ces caractéristiques permettent de différencier les pixels et de composer les images.



▲ IMG. 15

Chaque pixel peut prendre un certain nombre de couleurs déterminées par la palette qu'utilise l'image.

La couleur qui est affectée à un pixel est généralement obtenue par un mélange de rouge de vert et de bleu. On parle alors de *couleur RVB ou RGB en anglais*. Il existe cependant différentes manières de décrire les couleurs. Il est donc possible de *décomposer une couleur en cyan, magenta, jaune et noir (couleur CMJN ou CMYB en anglais)* ou encore *en teinte, saturation, luminosité (couleur LTS ou HSB en anglais)*. La palette de couleurs d'une image représente *l'ensemble des couleurs dont elle est constituée*. Plus précisément, c'est l'ensemble des couleurs que peuvent prendre les pixels de cette image. Les palettes de couleurs peuvent ne comporter que très peu de couleurs (2, 4, 8, ...) ou au contraire un nombre presque illimité (jusqu'à 16 millions de couleurs), pour les images à haute définition, comme par exemple les photographies.

Les peintres traditionnels utilisent des palettes sur lesquelles ils disposent les couleurs qui vont apparaître dans leurs tableaux. Les infographistes procèdent de la même manière avec les images numériques. Même si l'utilisation des palettes est, en partie automatisée, il est toujours possible de définir et d'attribuer un certain nombre de couleurs aux palettes numériques. Il existe plusieurs types de palettes de couleurs. Plus une palette possède de couleurs et plus elle offre de liberté à la création des images. En revanche, l'utilisation de palettes riches alourdit le poids des fichiers images correspondants.

Il existe donc *différents formats de fichiers images* sur le Web (*GIF* et *JPEG*) qui permettent, entre autre, de définir exactement le type de palette que l'on souhaite fournir aux images.

Le dernier paramètre qu'il est nécessaire d'ajuster lorsque l'on crée une image numérique est sa *résolution*. Il serait possible de comparer la résolution des images numériques, à la taille des grains d'une photo traditionnelle.



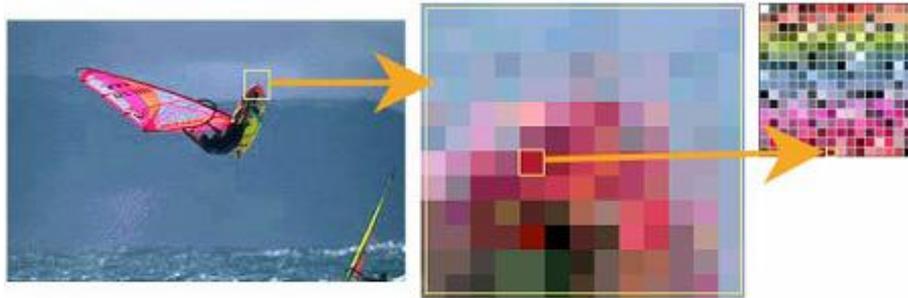
Les différents types de palettes

Les palettes de couleurs indexées

Chaque couleur peut être référencée dans une palette de couleurs. Les palettes, au sens informatique du terme, sont en réalité limitées à 256 couleurs. On parle alors de couleurs indexées. Elles sont utilisées par les fichiers de type GIF.

Dans ce cas, on ne précise pas les niveaux de rouge, de vert et de bleu qui donnent sa couleur au pixel, mais simplement la référence de cette couleur dans la palette. Cette astuce permet de *limiter la taille des fichiers de type image*.

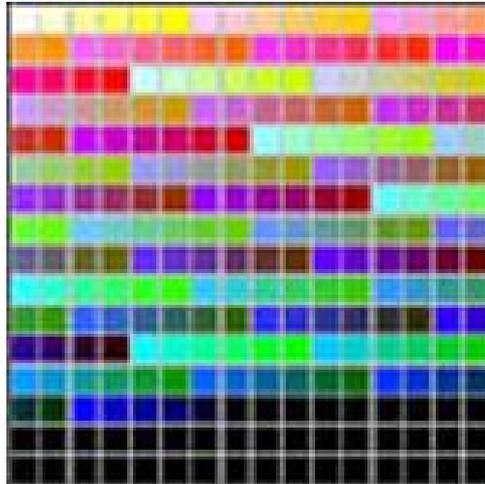
De plus, il est possible de *préciser le nombre de couleurs de la palette (de 2 à 256)*. Voilà la manière dont sont indexées les couleurs.



▲ IMG. 16 : LA COULEUR DU PIXEL ENCADRÉ EST LA COULEUR 207 DE LA PALETTE DE DROITE. - SPÉCIFIQUE

Un cas particulier, la palette Web

La palette WEB est une palette spéciale puisqu'elle ne s'utilise qu'avec des images diffusées sur le Web. La palette WEB en comprend 216. Ces 216 couleurs de cette palette s'affichent de la même façon sur les principaux navigateurs et systèmes d'exploitation.



▲ IMG. 17 : LA PALETTE WEB - SPÉCIFIQUE

◆ Pourquoi 216 couleurs ?

Chaque navigateur (ou browser en anglais) et chaque système d'exploitation (PC, MAC) dispose d'une palette de 256 couleurs qui lui permet d'afficher les images. Mais cette palette de 256 couleurs n'est pas universelle, chaque constructeur étant libre de définir cette palette à sa guise. Ces palettes présentent donc de légères nuances qui peuvent dégrader fortement l'affichage des images dans certains navigateurs.

Il existe toutefois un certain consensus lié à l'existence d'une sorte de standard HTML qui stipule qu'une certaine palette dite "palette web" (en anglais "safe-web palette" ou "safety palette") doit être privilégiée : dans les faits, la quasi totalité des navigateurs internet ("browsers" en anglais) respecte cette palette présentant les 216 couleurs communes aux principaux navigateurs.

Utiliser la palette WEB pour créer des images permet donc d'obtenir des images dont la qualité ne sera pas dégradée d'un navigateur à l'autre.

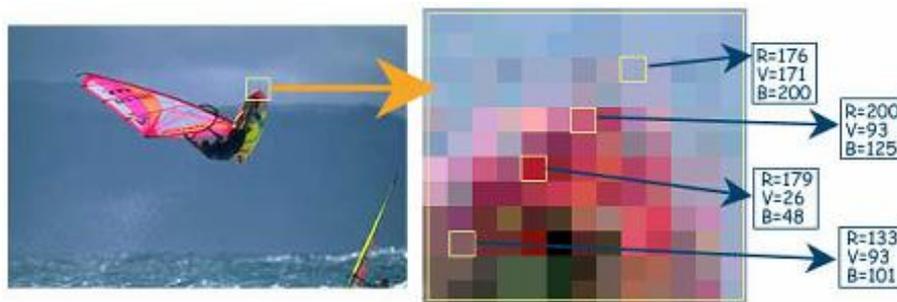
La plupart des logiciels de création de pages Web, éditeurs HTML (Dreamweaver, FrontPage, etc.) comprennent des outils facilitant l'utilisation de cette palette de 216 couleurs. Les logiciels graphiques (Fireworks, Flash, ImageReady, Photoshop, etc.) proposent, désormais, directement la palette Web dans la liste des diverses options de palettes à disposition.

Palettes de couleurs vraies

Passée cette limite de 256 couleurs, on utilise des *couleurs vraies*, ou par abus de langage une *palette de 16 ou 32 millions de couleurs*. C'est à dire que chaque couleur est décrite en *RVB* (Rouge, Vert, Bleu), *TLS* (Teinte, Luminosité, Saturation), ou *CMJN* (Cyan, Magenta, Jaune, Noir).

Référencer la couleur d'un pixel dans une telle palette ne ferait qu'augmenter la taille de l'image tant la palette est grande. On utilise donc un autre format de fichier pour les images appelé JPEG.

Voici comment sont décrites les couleurs pour une palette de 16 millions de couleurs (au format JPEG) : les composants *Rouge Vert* et *Bleu* de chaque pixel sont donnés avec précision.



▲ IMG. 18 : DESCRIPTION DES INFORMATIONS DE COULEURS D'UN PIXEL - SPÉCIFIQUE

Annexes

ANNEXE A

**Cadre Commun d'Interopérabilité
(CCI) - Septembre 2003**



Cadre commun d'interopérabilité
version 2.1
Mise à jour des standards et des référentiels

**Rapport de mise à jour des standards et
des référentiels proposé pour le Cadre
Commun d'Interopérabilité
Version 2.1
(septembre 2003)**

SOMMAIRE

1	<i>Justification des compléments et suppressions par rapport à la version 1 du CCI.....</i>	6
1.1	Le réseau et le transport de l'information.....	6
1.1.1	Les réseaux LAN/WAN.....	6
1.1.1.1	Protocoles IP.....	6
1.1.1.1.1	Standards applicables : IPv4.....	8
1.1.1.1.2	Candidats au référentiel Vx : IPv6.....	8
1.1.1.2	Protocole de transport.....	9
1.1.1.2.1	Standards applicables.....	9
1.1.1.2.2	Candidats au référentiel Vx.....	9
1.1.1.3	SSLv3/TLS.....	9
1.1.1.3.1	Standards applicables.....	10
1.1.1.4	IPSec.....	10
1.1.1.4.1	Standards applicables.....	10
1.1.1.5	Le protocole hypertexte.....	11
1.1.1.5.1	Standards applicables.....	11
1.1.1.6	Les transferts de fichiers.....	12
1.1.1.6.1	Standards applicables.....	12
1.1.1.6.2	Candidats au référentiel Vx.....	12
1.1.1.7	Les newsgroups.....	13
1.1.1.7.1	Candidats au référentiel Vx.....	13
1.1.1.8	Les protocoles de réseaux sans fil.....	13
1.1.1.8.1	Les principes du standard IEEE 802.11.....	14
1.1.1.8.2	Wi-Fi : évolution du standard IEEE 802.11.....	15
1.1.1.8.3	Wi-Fi : aspects sécurité.....	15
1.1.1.8.4	Tendances.....	16
1.1.1.8.5	Standards applicables.....	16
1.1.1.8.6	Candidats au référentiel Vx.....	16
1.2	Les services des systèmes d'information et de communication.....	17
1.2.1	L'adressage.....	17
1.2.1.1	DNS.....	17
1.2.1.2	DNSSec.....	17
1.2.1.3	Standards applicables.....	18
1.2.1.4	Candidats au référentiel Vx.....	18
1.2.2	Le format URI d'identification de ressources.....	19
1.2.2.1.1	Standards applicables.....	19
1.2.3	La messagerie.....	20
1.2.3.1	Le protocole SMTP.....	20
1.2.3.2	La sécurité de la messagerie électronique.....	21
1.2.3.2.1	MIME based secure EDI.....	21
1.2.3.2.2	S/MIME.....	21
1.2.3.2.3	Standards applicables.....	21
1.2.3.3	Extensions à la messagerie SMTP.....	22
1.2.3.3.1	Standards applicables.....	22
1.2.4	L'annuaire.....	23
1.2.4.1	Contexte d'introduction du protocole LDAP.....	23
1.2.4.2	Conséquences sur les standards.....	24
1.2.4.3	Les extensions de Sécurité.....	24
1.2.4.4	Standards applicables.....	27
1.2.4.5	Candidats au référentiel Vx.....	27
1.2.4.6	L'infrastructure à clé publique.....	28
1.2.4.6.1	PKI.....	28
1.2.4.6.2	Standards applicables.....	28

1.2.5	La qualité de service.....	29
1.2.5.1	Les standards de la Qualité de Service	29
1.2.5.1.1	Principes	29
1.2.5.1.2	Les tendances.....	30
1.2.5.1.3	Candidats au référentiel Vx.....	30
1.3	Intégration des données	31
1.3.1	Les langages XSLT et XPath	31
1.3.1.1	Tendances.....	31
1.3.1.2	Candidats au référentiel Vx	31
1.3.2	La sécurité XML	32
1.3.2.1	XML-Signature	32
1.3.2.2	XML-Encryption	33
1.3.2.3	XKMS	33
1.3.2.4	XACML	34
1.3.2.5	SAML.....	34
1.3.2.6	Standards applicables	34
1.3.2.7	Candidats au référentiel Vx.....	35
1.3.3	Le langage UML	35
1.3.3.1	Standards applicables	37
1.3.4	La méthodologie UN/CEFACT Modeling Methodology (UMM)	37
1.4	Formats des données numériques	39
1.4.1	Jeux de caractères et alphabets.....	39
1.4.2	Formats de documents.....	39
1.4.2.1	TXT	39
1.4.2.2	XML	39
1.4.2.3	SGML.....	39
1.4.2.4	HTML.....	39
1.4.2.5	RTF.....	40
1.4.2.6	PDF.....	40
1.4.2.7	XHTML.....	40
1.4.2.8	OASIS Open Office XML Format	40
1.4.2.9	Microsoft Office v11 XML Format.....	40
1.4.2.10	PDF/A	40
1.4.2.11	XForms	41
1.4.2.12	Candidats au référentiel Vx.....	42
1.4.3	Échange d'information graphique/images fixes.....	43
1.4.3.1	TIFF (UIT T4).....	43
1.4.3.2	PNG	43
1.4.3.3	GIF	43
1.4.3.4	JPEG.....	43
1.4.3.5	SVG.....	43
1.4.4	Flux audiovisuels	44
1.4.4.1	MP3	44
1.4.4.2	WAV	44
1.4.4.3	MPEG-2	44
1.4.4.4	MPEG-4	44
1.4.4.5	DV	44
1.4.4.6	Ogg Vorbis	45
1.4.4.7	AAF.....	45
1.4.4.8	MPEG-4 Part 10/ H26L.....	45
1.4.4.9	Candidats au référentiel Vx.....	45
1.4.5	Échange de bases de données.....	46
1.4.5.1	XML	46
1.4.5.2	CSV (texte plat).....	46

1.4.6	Plans.....	46
1.4.6.1	CGM.....	46
1.4.6.2	STEP.....	46
1.4.6.3	DXF.....	46
1.5	Les architectures applicatives	47
1.5.1	Les Services Web.....	47
1.5.1.1	Les Services Web et la sécurité.....	47
1.5.2	La technologie J2EE (le standard 1.3).....	49
1.5.3	La technologie .NET.....	50
1.5.4	La technologie ZOPE du monde des logiciels libres.....	51
1.5.4.1	Le modèle d'architecture de ZOPE.....	52
1.5.4.2	Les composants majeurs de ZOPE.....	52
1.5.4.2.1	ZServer.....	52
1.5.4.2.2	Zope Core.....	52
1.5.4.2.3	Base de données Objet (ZODB).....	53
1.5.4.2.4	Intégration SGBDR.....	53
1.5.4.2.5	Zope Products.....	53
1.5.4.2.6	ZClasses.....	53
1.5.4.3	L'architecture Zope et le respect des normes et standards ouverts.....	53
1.5.4.4	L'architecture ZOPE vis à vis des normes, standards et architectures du moment.....	54
1.5.5	Standards applicables.....	55
1.5.6	Candidats au référentiel Vx.....	55
2	Récapitulatif des mises à jour proposées pour la version 2 du CCI.....	57
2.1	Interconnectivité.....	57
2.1.1	Les standards proposés pour suppression.....	57
2.1.1.1	Suppression de standards du référentiel.....	57
2.1.1.2	Suppression de candidats aux versions ultérieures.....	57
2.1.2	Les standards proposés en complément.....	58
2.1.2.1	Compléments au référentiel courant.....	58
2.1.2.2	Complément de candidats aux versions ultérieures.....	59
2.2	Données.....	60
2.2.1	Les standards proposés pour suppression.....	60
2.2.1.1	Suppression de standards du référentiel.....	60
2.2.1.2	Suppression de candidats aux versions ultérieures.....	60
2.2.2	Les standards proposés en complément.....	60
2.2.2.1	Compléments au référentiel courant.....	60
2.2.2.2	Complément de candidats aux versions ultérieures.....	60
2.3	Formats et supports.....	61
2.3.1	Les standards proposés pour suppression.....	61
2.3.1.1	Suppression de standards du référentiel.....	61
2.3.1.2	Suppression de candidats aux versions ultérieures.....	61
2.3.2	Les standards dont l'Etat a subi une évolution.....	62
2.3.3	Les standards proposés en complément.....	63
2.3.3.1	Compléments au référentiel courant.....	63
2.3.3.2	Complément de candidats aux versions ultérieures.....	63
2.4	Les architectures applicatives	64
2.4.1	Les standards proposés en complément.....	64
2.4.1.1	Compléments au référentiel courant.....	64
2.4.1.2	Complément de candidats aux versions ultérieures.....	64
3	Conclusion.....	65



Cadre commun d'interopérabilité
version 2.1
Mise à jour des standards et des référentiels

3.1	Tableaux des standards intégrés dans la Version V2.1 du CCI	65
3.1.1	Interconnectivité.....	65
3.1.2	Données.....	66
3.1.3	Formats et supports	67
3.1.4	Architectures applicatives	68
3.2	Tableaux des standards « candidats » envisagés pour les Versions ultérieures du CCI.....	69
3.2.1	Interconnectivité.....	69
3.2.2	Données.....	69
3.2.2	Données.....	70
3.2.3	Formats et supports	71
3.2.4	Architectures applicatives	72



Cadre commun d'interopérabilité
version 2.1
Mise à jour des standards et des référentiels

1 Justification des compléments et suppressions par rapport à la version 1 du CCI

1.1 LE RESEAU ET LE TRANSPORT DE L'INFORMATION

1.1.1 Les réseaux LAN/WAN

1.1.1.1 Protocoles IP

Aujourd'hui validé au sein de la version 1 du Cadre Commun d'Interopérabilité, le protocole IPv4 se présente comme la référence de niveau réseau pour l'interconnexion entre le réseau local Ethernet d'un ministère et le réseau transport du programme ADER.

L'objet du présent chapitre est d'évaluer le bien fondé de la conservation de ce protocole par rapport à l'opportunité d'un positionnement sur l'avenir en s'orientant vers les nouvelles évolutions, standardisées sous l'appellation IPv6.

En effet, la version 4 du protocole IP est parfaitement stable et déployée universellement à travers le monde. Avec TCP, protocole de transport associé, elle est le standard de base de l'Internet. Ce standard présente toutefois quelques limites que nous rappelons brièvement :

- la capacité d'adressage, tant la croissance du réseau est importante du fait de son large succès (l'espace d'adressage devrait atteindre la saturation vers 2008-2010) ;
- l'insuffisance des mécanismes de configuration d'adresse en termes de simplicité et d'automatisation, frein notable aux développements futurs de l'Internet mobile (ex. UMTS) ;
- l'insuffisance des propriétés de qualité de service, notamment sur la priorité des flux temps réel ;
- l'absence de fonctions de sécurité intrinsèques.

La version 6 du protocole IP apporte des solutions sur ces sujets, solutions mises en œuvre par de nouvelles fonctionnalités largement décrites au sein de la version 1 du présent document.

La question de l'adoption de cette orientation ne se pose pas tant elle est inévitable. L'évolution du marché la rendra incontournable (croissance du réseau, développement de l'Internet mobile de masse, du multi-media...). Il s'agit plutôt de s'interroger sur le moment opportun de sa prise en considération.

En termes d'infrastructure, deux réseaux phares se positionnent sur cette dernière technologie : le réseau RENATER connectant plus de 600 sites de recherche et d'enseignement en France et à l'international et le réseau expérimental 6BONE issu du projet IPng (IP nouvelle génération) de l'IETF.

En ce qui concerne le réseau 6BONE, il s'agit d'un projet de collaboration mondiale (incluant opérateurs, fournisseurs d'accès et équipementiers) dont l'objet est d'expérimenter la mise en œuvre d'un réseau IPv6. Ce projet, établi en 1996, démarra par la création d'un réseau virtuel de *Tunneling*, encapsulant les paquets du protocole IPv6 dans des paquets IPv4. Actuellement, le réseau migre doucement vers des liens IPv6



Cadre commun d'interopérabilité

version 2.1

Mise à jour des standards et des référentiels

natifs. La stratégie de déploiement n'est pas soumise à des contraintes de délai. Elle a pour seule vocation d'acquérir de l'expérience en matière de déploiement réseau. France Télécom est impliqué dans le projet.

Pour ce qui est du réseau RENATER (Réseau National de Télécommunication pour la Technologie, l'Enseignement et la Recherche), la technologie IPv6 a été déployée comme service expérimental bâti sur l'infrastructure ATM de RENATER 2. Ce pilote a succédé au G6-bone, issu du projet français G6, dont il a acquis l'expérience. Baptisé RENATER 3, il propose un accès double pile : les équipements traitent indifféremment les paquets IPv4 et les paquets IPv6. Il est connecté au réseau 6BONE. Le service IPv6 est actuellement disponible en chaque point de présence régional de l'épine dorsale du réseau RENATER 3. Il sert actuellement d'expérimentation, principalement pour la recherche.

En termes de produits, des couches protocolaires IPv6 sont disponibles pour la plupart des systèmes d'exploitation (ex. AIX, HP-UX, Linux, Windows NT 4/2000/XP), ainsi que pour les routeurs.

Mais il n'existe pas encore vraiment d'applications à ce jour nécessitant les nouvelles fonctionnalités. Ainsi, les opérateurs ne sont pas poussés par le marché pour développer activement leurs services.

L'Asie est toutefois très motivée par le passage à IPv6 dans la mesure où elle manque cruellement d'adresses IPv4. L'Europe est également motivée par l'explosion du marché des équipements mobiles, mais nous dépassons là le cadre du présent chapitre.

En ce qui concerne l'interconnexion LAN/WAN du réseau SETI (service de transport inter administration), il est prématuré de se positionner dès à présent vis-à-vis d'une migration IPv6, dans la mesure où les opérateurs ne sont pas prêts à rendre le service au public en l'absence d'un marché réellement émergent.

Gageons tout de même que la migration du réseau sera longue et lourde en investissements. Elle s'effectuera pas à pas, l'infrastructure IPv4 côtoyant des niches d'évolution IPv6 selon les besoins.

Aujourd'hui nous n'en sommes pas là. La suggestion de suivre de près les évolutions du marché avant d'entreprendre quoi que ce soit dans ce domaine, suggestion effectuée au sein de la version 1 du présent document, est toujours d'actualité. Il est donc conseillé de reconduire le référentiel à l'identique pour la présente version 2 et d'attendre d'entrevoir un réel besoin avant d'envisager une interopérabilité avec IPv6.

Le référentiel prévisionnel IPv6 peut toutefois être agrémenté de nouvelles fonctionnalités, dans la mesure où certaines d'entre elles, non référencées jusqu'à présent, peuvent présenter un grand intérêt pour l'avenir.

Par exemple, la recommandation RFC 2675 est intéressante dans la mesure où elle propose la possibilité d'émettre des paquets supérieurs à 65 Ko, limite jusque là établie par la conception des protocoles TCP/IP. Le dépassement de cette limite permet alors d'émettre de plus gros paquets sur les réseaux de type haut débit, de manière à accroître les performances aux nœuds d'interconnexion sur les transferts de données en masse.

En effet, IPv6 permettant d'introduire des options de longueur variable au sein de l'en-tête de ses paquets, la limite des 65 Ko de données n'est plus infranchissable. La recommandation RFC 2675 définit alors 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.

Actuellement au stade de standard proposé, cette recommandation devra être prise en considération si elle est suivie des éditeurs et opérateurs. Elle est ainsi proposée au référentiel prévisionnel du cadre commun d'interopérabilité dans un but de suivi et de veille technologique.

1.1.1.1.1 Standards applicables : IPv4

STANDARD	RFC	DATE	ETAT	REMARQUES
IP V4	791	Sept-81	Standard	

1.1.1.1.2 Candidats au référentiel Vx : IPv6

Le référentiel IPv6, n'ayant pas subi d'évolution concernant les RFCs majeures, est reconduit à l'identique, à l'exception de la recommandation RFC 2675.

STANDARD	RFC	DATE	ETAT	REMARQUES
IPv6	2373	Juillet-98	Proposé	Architecture d'adressage IP V6
	2374	Juillet-98	Proposé	Format d'adressage unicast IP V6
	2460	Déc-98	Draft	Spécification
	2461	Déc-98	Draft	Gestion de l'environnement
	2462	Déc-98	Draft	Autoconfiguration
	2463	Déc-98	Draft	ICMP V6
Ipv6 TCP/UDP	2675	Août-99	Proposé	Augmentation du volume des paquets
Transition IP.V4 -> IP.V6	2893	Août-00	Proposé	
Transition IP.V4 -> IP.V6	2766	Fév-00	proposé	

1.1.1.2 Protocole 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 standards n'ont pas beaucoup évolué depuis leurs spécifications de base. 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 en standard, telles que référencées au sein de la version 1 du présent document.

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. Elle est recommandée pour la présente version, à titre d'option.

1.1.1.2.1 Standards applicables

STANDARD	RFC	DATE	ETAT	REMARQUES
TCP	793	sept-81	Standard	Standard MIL-STD-1778
UDP	768	août-80	Standard	Imposer des contraintes de sécurité
TCP	1323	Mai-92	Proposé	Améliore les performances haut débit

1.1.1.2.2 Candidats au référentiel Vx

Les futures recommandations à intégrer concernent les améliorations apportées à TCP. Ces améliorations, actuellement à l'état proposé, ne sont pas suffisamment stables en termes de produits pour pouvoir les inclure dès maintenant au sein du référentiel du cadre commun d'interopérabilité.

STANDARD	RFC	DATE	ETAT	REMARQUES
TCP	2018	Oct-96	Proposé	Acquittement sélectif des données
TCP	2581	Avril-99	Proposé	Contrôle de congestion (mis à jour par la RFC 3390)
TCP	2873	Juin-2000	Proposé	Gestion de la priorité IPv4
TCP	2883	Juillet-2000	Proposé	Extension à l'acquittement sélectif
TCP	3042	Janv-2001	Proposé	Nouveau mécanisme pour améliorer la gestion de perte de données
TCP	3168	Sept – 2001	Proposé	Notification explicite de congestion
TCP	3390	Oct-2002	Proposé	Augmentation de la fenêtre initiale
IPv6 TCP/UDP	2675	Août- 99	Proposé	Cf. § 1.1.1.1

1.1.1.3 SSLv3/TLS

SSL est un protocole de communication sécurisé qui propose plusieurs services de sécurité :

- Authentification des parties communicantes par utilisation de certificats X.509v3 pour le serveur (à partir de la version 2) et pour le client (à partir de la version 3) ;
- Intégrité et confidentialité des échanges (scellement et chiffrement) ;
- Unicité de la session (les informations d'authentification ne sont pas rejouables).

Conçu à l'origine par Netscape pour la sécurité des échanges entre client et serveur Web, SSL est aujourd'hui incontournable dès que l'on évoque la sécurité d'une connexion. Ce protocole peut utiliser différentes technologies cryptographiques dont : DES, 3DES, RC2/RC4, RSA, MD5, SHA, Diffie&Hellman, etc.

SSL présente l'avantage d'être un protocole de niveau transport indépendant des protocoles de niveau applicatif, et permet ainsi de garantir la sécurité de nombreux services TCP : HTTPS (port 443), SMTPS (port 465), IMAPS (port 993), NNTPS (port 563), LDAPS (port 636), etc.

SSL est désormais un standard du marché qui évolue dans le cadre IETF du Transport Layer Security (TLS) Working Group.

Le protocole TLS 1.0 est basé sur le protocole de sécurité SSL 3.0 mais ces deux protocoles par leurs différences ne sont pas interopérables entre eux.

1.1.1.3.1 Standards applicables

STANDARD	RFC	DATE	ETAT	REMARQUES
SSLv3/TLS	2642	Jan-99	Proposé	

1.1.1.4 *IPSec*

Le sujet IPSec est largement couvert dans le « Rapport de validation des standards et des référentiels figurant dans le cadre commun d'interopérabilité – Première version ». De plus, du point de vue standard, aucune modification notable n'est à signaler par rapport au CCI v1.

1.1.1.4.1 Standards applicables

STANDARD	RFC	DATE	ETAT	REMARQUES
IPSec	2401 à 2410	Nov-98	Proposé	
	2411 et 2412	Nov-98	Informationnel	

1.1.1.5 Le protocole hypertexte

Le protocole HTTP (Hypertext Transfer Protocol) est la référence en matière de transmission de données en contexte Web. Il permet à un client, via son logiciel navigateur Internet, d'effectuer des transactions avec un serveur de contenu Web.

Ce protocole, très largement utilisé, est devenu la référence incontournable pour les raisons suivantes :

- il est indépendant de la plate-forme matérielle et du système d'exploitation sous-jacent ;
- il permet l'échange de paramètres divers, notamment du formatage de l'information, de manière suffisamment souple pour répondre à une large étendue de besoins sans avoir à configurer spécifiquement la partie logicielle cliente.

Le protocole existe actuellement en deux versions : la version 1.0 relatif aux spécifications de base et la version 1.1 apportant des améliorations, telles que la possibilité de définir plusieurs noms de domaine par serveur, la persistance des connexions, une meilleure gestion du cache et la sécurité.

La version 1.1 étant devenue la référence des deux leaders du marché en matière de navigateurs Internet d'une part (Internet Explorer de Microsoft et Navigator de Netscape), la spécification de cette version ayant été définie pour permettre la compatibilité ascendante avec la version précédente d'autre part, seule la version 1.1 est actuellement référencée au sein du cadre commun d'interopérabilité.

L'IETF travaille actuellement à l'élaboration d'extensions pour des besoins spécifiques. La définition de ces extensions, concentrée dans la recommandation RFC 2774, était d'abord soumise à l'IETF comme standard proposé. Mais, du fait du manque de consensus entre les intervenants, elle a finalement été publiée comme standard expérimental. A ce stade, il est trop tôt pour prévoir son introduction dans une quelconque version du référentiel commun d'interopérabilité.

Ainsi, les standards applicables à la version 2 du cadre commun d'interopérabilité sont inchangés par rapport à la version précédente.

1.1.1.5.1 Standards applicables

STANDARD	RFC	DATE	ETAT	REMARQUES
HTTP V1.1	2616	Juin-99	Draft	Spécification de la version 1.1
HTTP V1.1	2817	Mai-2000	Proposé	Mise à jour incluant la fonction TLS de sécurité

1.1.1.6 Les transferts 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.

Sa simplicité, décrite au sein de la version 1 du présent document, en fait sa limitation et ainsi son défaut. Mais actuellement toujours largement utilisé, principalement hors contexte Web, le protocole FTP est sujet à des améliorations à prendre en considération. D'ailleurs, les améliorations en termes d'extensions de sécurité (RFCs 2228 et 2773) et d'internationalisation (prise en compte du codage UTF-8 dans le RFC 2640) ont déjà été prises en compte au sein du référentiel commun d'interopérabilité.

Pour être complète, la liste des recommandations doit comprendre le RFC 2389, recommandation permettant de découvrir les options supportées par l'application distante afin de pouvoir les négocier pour utilisation. Il est ainsi conseillé d'ajouter cette recommandation au référentiel existant.

D'autre part, des extensions sont prévues pour interopérer avec le protocole IPv6. Il est dans ce cas logique de les proposer pour une version ultérieure du référentiel commun d'interopérabilité, lorsque requis.

1.1.1.6.1 Standards applicables

STANDARD	RFC	DATE	ETAT	REMARQUES
FTP	959	octobre-85	Standard	Spécification de base
	2228	octobre-97	Proposé	Extensions de sécurité
	2640	juillet-99	Proposé	Extension aux codes internationaux
	2773	février-00	Expérimental	Mécanismes d'authentification
	2389	août-98	Proposé	Négociation des options

Rappelons que l'utilisation de ce protocole est déconseillée en contexte Web, dans la mesure où le protocole HTTP remplit la fonction et qu'il est destiné à se substituer à FTP dans un proche avenir.

1.1.1.6.2 Candidats au référentiel Vx

STANDARD	RFC	DATE	ETAT	REMARQUES
FTP	2428	sept-98	Proposé	Extensions pour IPv6 et NATs

1.1.1.7 Les newsgroups

Il peut être intéressant d'élaborer des groupes de discussions, via l'Internet, sur des sujets d'intérêt commun. Le protocole NNTP (Network News Transfer Protocol) est proposé à cet effet.

Proposé pour standardisation à l'IETF en 1986, largement utilisé et n'ayant pas subi d'évolution depuis sa spécification initiale, ce protocole présente incontestablement les critères d'interopérabilité requis.

L'objet du présent chapitre est de le faire apparaître dans le cadre d'une version ultérieure, de manière à faire ressortir l'expression d'un éventuel besoin conduisant à l'introduction du protocole au référentiel.

Il est à noter que la recommandation RFC 2980 est supprimée au sein de la présente version du document dans la mesure où son statut n'est qu'informationnel. A ce titre, la recommandation n'a pas vocation de devenir un standard et n'a donc pas à figurer au référentiel.

1.1.1.7.1 Candidats au référentiel Vx

STANDARD	RFC	DATE	ETAT	REMARQUES
NNTP	977	février-86	Proposé	Spécification du protocole

1.1.1.8 Les protocoles de réseaux sans fil

Après avoir connu un succès considérable avec la téléphonie mobile, les technologies sans fil s'appliquent désormais aux réseaux locaux avec les WLAN (*Wireless Local Area Network*). Ces technologies émergentes connaissent actuellement un succès certain. Aussi, l'objet du présent chapitre est de dégager les standards applicables sur un marché d'ors et déjà incontournable.

En premier lieu, notons qu'il existe actuellement deux standards de réseaux locaux sans fil : le standard HiperLAN (*High Performance Radio Lan*), issu du projet BRAN (*Broadband Radio Acces Network*) de l'ETSI (*European Telecommunications Standards Institute*), et le standard 802.11 de l'IEEE (*Institute of Electrical and Electronics Engineers*). Ces deux standards étant issus de deux organismes de standardisation différents, sont incompatibles entre eux.

Le standard HyperLAN définit deux types de réseau, HiperLAN 1 et HiperLAN 2, utilisant tous deux la bande de fréquence de 5 GHz. HiperLAN 1 offre des débits de 10 et 20 Mb/s. HiperLAN 2 atteint 54 Mb/s.

Ce standard HyperLAN n'en est actuellement qu'au stade de prototype et il n'existe pas à ce jour de produits commercialisés. En concurrence directe avec le standard 802.11, lui même opérationnel et déjà fortement commercialisé, le standard HyperLAN n'est pas assuré de voir le jour. Il n'est donc pas raisonnable de considérer aujourd'hui le standard HyperLAN pour un quelconque référentiel du CCI. Ainsi, nous ne prendrons en considération au sein de ce chapitre que le standard 802.11.

1.1.1.8.1 Les principes du standard IEEE 802.11

Ce standard s'apparente à Ethernet dans la mesure où il définit deux couches de liaison de données, les couches LLC (*Logical Link Control*) et MAC (*Medium Access Control*), comme pour Ethernet, ainsi qu'une couche physique qui, elle, répond aux besoins spécifiques d'une communication sur ondes hertziennes.

La couche LLC a été définie initialement par le standard IEEE 802.2. Cette couche permet d'établir un lien logique entre la couche MAC et la couche réseau (niveau 3 du modèle OSI). Ce lien permet de rendre interopérable des réseaux complètement différents dans la conception de la couche physique ou de la couche MAC, mais possédant la même couche LLC. La couche LLC fournit deux types de fonctionnalités : le contrôle de flux et la reprise sur erreur. Celle définie dans le standard 802.11 utilise les mêmes propriétés que celle du 802.2, de manière à être compatible avec n'importe quel autre réseau de ce type, tel Ethernet.

Le rôle de la couche MAC est assez similaire à celui d'Ethernet (standard IEEE 802.3). Cette couche assure la gestion de l'accès de plusieurs stations à un support partagé où chaque station écoute avant d'émettre. La différence notable avec la couche MAC d'Ethernet se situe sur la gestion des collisions. En effet, Ethernet assure la détection des collisions en cours de transmission, ce qui n'est pas possible dans les systèmes radio. Dans ce dernier cas, la transmission sur une fréquence donnée empêche la station d'écouter sur cette même fréquence. Des mécanismes d'évitement et de contrôle des collisions sont alors mis en œuvre, basés entre autre sur la réservation d'un temps de transmission et l'acquiescement des données.

Quant à la couche physique, elle peut être de trois types différents dans le standard 802.11 d'origine :

- FHSS (*Frequency Hopping Spread Spectrum*), basé sur l'étalement de spectre par saut de fréquence ;
- DSSS (*Direct sequence Spread Spectrum*), basé sur l'étalement de spectre, mais sur séquence directe ;
- IR (*InfraRed*), de type infrarouge.

Étant donné leurs caractéristiques, ces trois types de gestion de la couche physique sont incompatibles entre eux. Ainsi, deux cartes réseau de types différents ne peuvent dialoguer. Notons tout de même que les deux techniques de transmission sur onde radio (FHSS et DSSS) utilisent la même bande de fréquence (2,4 GHz).

Remarquons finalement que les principes énoncés ci-dessus permettent de définir un réseau de type Ethernet sur faisceaux hertziens. Il est alors possible de connecter directement des stations entre elles par voie hertzienne, voire des équipements de type PDA, ainsi que d'établir des passerelles avec les réseaux fixes, notamment le réseau local Ethernet pour lequel le standard 802.11 est particulièrement bien adapté.

1.1.1.8.2 Wi-Fi : évolution du standard IEEE 802.11

Comme Ethernet, le standard 802.11 n'est pas figé et de nombreuses améliorations ont été apportées au standard d'origine. Ainsi existent actuellement trois standards majeurs :

- IEEE 802.11b, ou Wi-Fi, amélioration du 802.11 DSSS et utilisant la même bande de fréquence que le standard d'origine (2,4 GHz), permettant d'atteindre des débits de 11 Mb/s ;
- IEEE 802.11a, ou Wi-Fi5, utilisant une bande de fréquence de 5 GHz et pouvant atteindre 54 Mb/s ;
- IEEE 802.11g, compatible 802.11b et pouvant atteindre des débits de 54 Mb/s.

En matière d'interopérabilité, les produits correspondants sont soumis à des tests d'interopérabilité et à une certification de la part d'une association, la Wi-Fi alliance, regroupant les principaux acteurs du marché du sans fil et du monde informatique. Cette association regroupe actuellement plus de 200 compagnies et ont décerné la certification d'interopérabilité à plus de 600 produits.

Mais, pour prendre en considération l'un ou l'autre de ces standards, il est nécessaire de prendre en compte non seulement les éléments de marché et d'interopérabilité, mais aussi les contraintes d'utilisation.

En effet, l'utilisation des bandes de fréquence est régie par des organismes propres à chaque pays. L'ART (*Autorité de Régulation des Télécommunications*) la réglemente en France. Ainsi, la réglementation en vigueur en 2002 empêchait l'utilisation de la bande de fréquence de 5 GHz en extérieur. Quant à la bande de fréquence de 2,4 GHz, elle n'était autorisée que sur un domaine privé intérieur ou extérieur.

Or, un arrêté ministériel du 23 décembre 2002 a homologué une décision de l'ART, visant à assouplir ces règles de manière à pouvoir rendre un service Wi-Fi au public (de type 802.11b) dans les lieux de passage, tels les gares, les aéroports, les centres d'affaires ... Cet assouplissement, soumis dans de nombreux cas à autorisation, a été publié au journal officiel de 19 janvier dernier. Il est donc applicable depuis le 20 janvier. Ainsi, le standard 802.11b est applicable à la version 2 du CCI, selon les conditions précisées par la décision n° 2002-1008 de l'ART, décision homologuée par l'arrêté ministériel du 23 décembre 2002. Concernant le standard 802.11a, il est de fait exclu du référentiel CCI tant qu'il ne dispose pas des autorisations suffisantes pour pouvoir être utilisé par une administration. Quant au standard 802.11g, trop récent pour être pris en compte par l'ART (le standard a été finalisé récemment) et pour garantir la certification des produits (les premiers produits sortent tout juste en 2003), il pourra être intégré dans une version x à venir.

1.1.1.8.3 Wi-Fi : aspects sécurité

La sécurité est le point faible des réseaux Wi-Fi, du fait de leur caractère sans fil. Trois mécanismes de sécurité sont donc mis en œuvre pour tenter de pallier ce défaut :

- SSID (*Service Set Id*), identificateur du réseau à fournir lorsque l'on veut entrer dans un réseau ;
- ACL (*Acces Control List*), liste des adresses autorisées sur le réseau (adresses MAC des cartes réseau) ;
- WEP (*Wired Equivalent Privacy*), chiffrement destiné à l'intégrité et la confiance du dialogue.

Ces mécanismes sont toutefois vulnérables et il existe des techniques pour les contourner. Il est conseillé en attendant les améliorations à venir (cf. § 1.1.1.8.4), de sécuriser les réseaux Wi-Fi comme pour un réseau fixe, en mettant en œuvre des serveurs d'authentification (type Radius) et des tunnels de chiffrement (type IPsec).

1.1.1.8.4 Tendances

Les travaux en cours concernent principalement des améliorations de qualité de service (802.11e), d'interopérabilité entre points d'accès (802.11f) et du système de sécurité et d'authentification (802.11i).

Concernant la sécurité, des améliorations conséquentes sont attendues courant 2003. Elles concernent une nouvelle fonctionnalité appelée WPA (*Wi-Fi Protected Access*). Issue du projet de standard 802.11i, cette fonctionnalité devrait être commercialisée comme mise à jour logicielle pour les cartes réseau existantes.

1.1.1.8.5 Standards applicables

STANDARD	Standard IEEE	DATE	ETAT	REMARQUES
Wi-Fi	802.11b	2000	Standard	Version actuellement déployée

1.1.1.8.6 Candidats au référentiel Vx

STANDARD	Standard IEEE	DATE	ETAT	REMARQUES
Wi-Fi	802.11g	2000	Std Project	Version émergente (débit 54 Mb/s)
	802.11i	2001	En cours	Intégration de la sécurité WPA

1.2 LES SERVICES DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

1.2.1 L'adressage

1.2.1.1 DNS

Le service de nom de domaine DNS (*Domain Name Server*) a pour vocation d'effectuer le lien entre une adresse Internet au format alphanumérique et son adresse réseau effective, adresse IP numérique sur 32 bits. Ce service peut être vu comme une base de données distribuées dans l'Internet.

La version 1 du présent document référence les standards de base de ce service, standards que nous ne remettons pas en cause au sein de la présente version, tant il existe de recommandations complémentaires, récentes pour la plupart, nuisant à la visibilité en matière d'interopérabilité.

Toutefois, dans un souci de cohérence avec les mises à jour proposées dans les autres domaines, il est souhaitable de pouvoir disposer d'une première vision de l'évolution du DNS prévue pour IPv6. En effet, dans ce cadre, le service de nom de domaine est l'un des premiers acteurs concernés dans la mesure ou il gère des adresses IP, adresses dont le format et la gestion en IPv6 diffèrent de ceux d'IPv4.

Ainsi, la recommandation RFC 1886 définit des extensions au DNS permettant d'intégrer le format et la dynamique de gestion des adresses IPv6. Cette recommandation, actuellement au stade proposé, est suivie de recommandations informatives et de pratiques courantes ne donnant pas lieu à des standards. Aussi, bien que la stabilité de la recommandation de base ne soit pas établie, il est conseillé dès à présent de prévoir son inclusion dans un référentiel à venir, de manière à faciliter le suivi de son évolution.

1.2.1.2 DNSSec

Le DNS est le service de base indispensable dès lors que l'on souhaite accéder à l'Internet. En effet, toute 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, aussi étonnant que cela puisse paraître, le service DNS est l'un des moins sécurisé par nature et ses diverses implémentations (dont la plus connue est Bind) ont essuyé par le passé une myriade de vulnérabilités largement exploitées par les pirates. Si l'on ajoute à cela les mauvaises installations du DNS¹, nous comprenons pourquoi le service DNS est l'un des vecteurs favoris d'intrusion des systèmes d'information. Ainsi, on ne compte plus les attaques du DNS de type déni de service, usurpation ou inondation recensées par le SANS Institute ou les différents CERT de par le monde. 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 de réseau, avec les conséquences économiques que l'on imagine tant ce dernier est devenu en quelques années un élément incontournable de l'activité de nombreuses entreprises dans le monde.

Ce n'est que très récemment (au regard de l'apparition du DNS) que des extensions sécurité pour le DNS sont apparues 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.

¹ La campagne de nettoyage de printemps 2000 menée par Iperformances a montré que 30% des serveurs DNS de la zone .fr présentaient des défauts de configuration, pourcentage qui monte à 80% pour la zone .com.

Cependant, même si l'adoption de DNSSec en tant que standard paraît aujourd'hui inévitable à terme, son adoption sur le terrain prendra du temps. En attendant, de nombreux projets² 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 du standard, les travaux portent essentiellement sur l'optimisation du support de DNSSec, que ce soit au niveau des performances (RFC 3226) ou de la facilité de mise en œuvre (RFC 3445).

1.2.1.3 Standards applicables

STANDARD	RFC	DATE	ETAT	REMARQUES
DNS	1034	Nov-87	Standard	
	1035	Nov-87	Standard	
	1101	avril-89	Non indiqué	Actualise les RFC 1034 et 1035
	2535	mars-99	Proposé	
DNSSec	2535	Mar-99	Proposé	Extension sécurité DNS
	2931	Sept-00	Proposé	Mise à jour de la signature des requêtes et réponses DNS
	3007	Nov-00	Proposé	Sécurisation des mises à jour DNS
	3008	Nov-00	Proposé	Autorité de signature DNSSec

1.2.1.4 Candidats au référentiel Vx

STANDARD	RFC	DATE	ETAT	REMARQUES
DNS	1886	Déc-95	Proposé	Extensions pour le support IPv6
DNSSec	3226	Déc-02	Proposé	Support des enregistrements DNSSec et des adresses IPv6
	3445	Déc-02	Proposé	Limitation du champ d'action du Ressource Record KEY

² NAI Labs, NIST, RIPE, Verisign et notamment SECREG, démarré en Novembre 2002 pour une durée d'un an, dont les objectifs sont d'acquérir un savoir-faire sur la façon d'introduire DNSSec dans un TLD (*Top Level Domain*) comme .nl, de tester les procédures DNSSec et de former les administrateurs à DNSSec.

1.2.2 Le format URI d'identification de ressources

Ce chapitre concerne l'identification des ressources de l'Internet. Le standard de base développé dans ce domaine est l'URL (*Uniform Resource Locator*). Il s'agit d'un moyen pratique permettant à une personne ou une application d'adresser les ressources de l'Internet par des méthodes d'accès protocolaires variées, selon un standard de format relativement intuitif. Par exemple, adresser l'URL <http://www.adae.pm.gouv.fr> signifie que l'on cherche à atteindre, via le protocole HTTP, les ressources Web de l'ADAE sous la direction du premier ministre du gouvernement français.

L'inconvénient principal de ce standard est d'associer directement l'identificateur aux caractéristiques d'accès à la ressource (méthode d'accès et emplacement de la ressource). Quand les caractéristiques d'une ressource changent, son URL n'est plus valable. Cette particularité peut apporter quelques soucis aux personnes habituées à solliciter la ressource ou, pire encore, aux applications qui la recensent.

Le standard URI (*Uniform Resource Identifier*) a été développé principalement pour pallier ce défaut. Il définit un format universel d'identification abstraite de la ressource, de manière à rendre cette identification indépendante des caractéristiques d'accès proprement dits. L'identification devient ainsi permanente.

Le référentiel MAIA (*service de Méta Annuaire Inter Administration*) de l'ADAE invoque l'utilisation du format d'attribut URI (RFC 2079) pour la référence de site portail au sein de l'annuaire LDAP. La cohérence impose alors de faire figurer la recommandation URI (RFC 2396) au sein du référentiel du cadre commun d'interopérabilité.

1.2.2.1.1 Standards applicables

STANDARD	RFC	DATE	ETAT	REMARQUES
URI	2396	Août-98	Draft	L' <i>Unique Resource Identifier</i> permet d'unifier la recherche d'informations

1.2.3 La messagerie

1.2.3.1 Le protocole SMTP

Le protocole SMTP (*Simple Mail Transfer Protocol*) permet le transfert du courrier électronique selon un procédé efficace et fiable, basé sur le transport TCP et donc conforme à IP.

Les standards de base sont référencés par les recommandations RFC 821 pour la spécification de base et RFC 822 pour le format des messages Arpanet. Cependant, ces standards ont été révisés en 2001 et ont ainsi été remplacés par les deux recommandations suivantes :

- RFC 2821 pour la spécification de base,
- RFC 2822 pour le format des messages.

Ainsi, les références officielles sont actuellement celles des recommandations RFC 2821 et RFC 2822.

En ce qui concerne la recommandation RFC 2821, elle reprend la spécification de base définie par la recommandation RFC 821, en prenant bien garde à ne pas ajouter de fonctionnalité, ni en modifier. Cette précaution permet d'assurer la compatibilité ascendante. Par ailleurs, la recommandation apporte des clarifications et impose quelques restrictions. La plupart des systèmes de messagerie adhèrent à cette norme.

Quant à la recommandation RFC 2822, elle définit l'en-tête et le corps du message proprement dit, constitué de texte codé en ASCII anglais.

Cette dernière spécification est un peu pauvre face aux formats utilisés de nos jours, tels que les images, les fichiers binaires ou les messages imbriqués. De plus, la spécification ne supporte pas les jeux de caractères non ASCII, ce qui peut poser problème ; en particulier pour des pays tels que la Russie ou le Japon.

Toutefois, le standard MIME (*Multipurpose Internet Mail Extensions*) vient combler ces lacunes en définissant comment coder les textes non ASCII et les attachements, de sorte qu'ils puissent être véhiculés au sein du standard RFC 2822. Les recommandations correspondantes (RFC 2045 à 2049) sont incluses au référentiel de messagerie inter administration de l'ADAE.

Notons aussi que la recommandation RFC 2821 prévoit l'utilisation éventuelle du codage MIME et de son extension 8 bits, ainsi que des extensions SMTP (la recommandation RFC 1869 d'extension SMTP est rendue obsolète par le RFC 2821).

1.2.3.2 *La sécurité de la messagerie électronique*

1.2.3.2.1 MIME based secure EDI

La messagerie électronique est l'application la plus utilisée quotidiennement sur l'Internet avec plus d'un milliard de messages envoyés par jour.

Avec l'avènement des technologies et des infrastructures réseau dites « TCP/IP », nombreuses sont les applications qui tentent d'en tirer partie afin d'offrir un nouveau moyen d'échange à leurs utilisateurs. Parmi elles, les applications EDI (Electronic Data Interchange) peuvent désormais utiliser SMTP afin d'échanger de façon sécurisée des données structurées.

1.2.3.2.2 S/MIME

Défini en 1995 par plusieurs éditeurs de logiciels pour résoudre les problèmes liés à l'interception et à la création de faux messages électroniques, le protocole S/MIME permet aujourd'hui d'échanger très simplement des courrier électroniques sécurisés.

S/MIME (Secure Multi-purpose Internet Mail Extension), actuellement dans sa version 3.0, définit un protocole ajoutant la signature numérique et le chiffrement au format MIME (RFC 1847), format structurant le corps d'un message électronique sur l'Internet.

S'appuyant sur les notions de signature et d'enveloppe électronique, S/MIME permet d'offrir les services d'authentification, de confidentialité, d'intégrité et de non-répudiation nécessaires à la sécurisation des applications de messageries. Plus généralement, S/MIME sécurise tout échange orienté message, comme par exemple les échanges de données informatisés (EDI).

Cette sécurisation des messages peut être mise en œuvre de bout en bout, c'est-à-dire entre l'émetteur du message et le destinataire ou bien entre deux serveurs de messagerie

1.2.3.2.3 Standards applicables

STANDARD	RFC	DATE	ETAT	REMARQUES
SMTP	2821	Avril 01	Proposé	Se substitue au RFC 821
SMTP ARPA	2822	Avril-01	Proposé	Se substitue au RFC 822
	2156	Janvier-98	Proposé	
MIME	3335	Sep-02	Proposé	Echange de messages EDI avec MIME
S/MIME	2632	Juin-99	Proposé	Support des certificats dans S/MIME v3
	2633	Juin-99	Proposé	Spécification des messages S/MIME v3
	2634	Juin-99	Proposé	Services de sécurité étendus pour S/MIME
	3369	Aou-02	Proposé	Définit la syntaxe pour signer, condenser, authentifier ou chiffrer le contenu d'un message
	3370	Aou-02	Proposé	Définit les conventions d'utilisation des algorithmes de cryptographie

1.2.3.3 Extensions à la messagerie SMTP

Des extensions au protocole SMTP ont été proposées dans le cadre de la version 1 du présent document.

Parmi ces extensions, certaines d'entre elles n'ont pas (ou plus) à figurer au référentiel, à savoir :

- la recommandation RFC 1869 est à supprimer dans la mesure où elle est rendue obsolète par la recommandation SMTP de référence (RFC 2821) ;
- la recommandation RFC 1428 n'a pas à figurer dans une quelconque version du référentiel dans la mesure où elle a le statut d'information. Elle n'a donc pas vocation de devenir un standard.

En revanche, d'autres recommandations, telles les recommandations RFC 1870 et 2920, peuvent être incluses au référentiel dans la mesure où elles ont acquis le statut de standard.

1.2.3.3.1 Standards applicables

STANDARD	RFC	DATE	ETAT	REMARQUES
E SMTP	1652	juillet-94	Draft	Le RFC 1652 définit une extension au protocole SMTP afin qu'il puisse supporter nativement des messages 8 bits-MIME par rapport à un usage conventionnel sur 7-bits (transport 8 bits entre MTA).
E SMTP	1891	janvier-96	Proposé	
E SMTP	1892 à 1894	janvier-96	Proposé	
E SMTP	1870	Sept-97	Standard	
E SMTP	2920	Set-2000	Standard	

1.2.4 L'annuaire

La question d'interopérabilité des données entre annuaires se pose depuis fort longtemps. Pour comprendre l'enjeu des évolutions actuelles, un bref historique s'impose avant d'aborder la problématique LDAPv3.

1.2.4.1 Contexte d'introduction du protocole LDAP

Le premier protocole d'annuaire destiné à l'interopérabilité entre systèmes hétérogènes (dits systèmes ouverts) a été défini par l'organisme de standardisation ISO (*International Standard Organization*).

L'ISO a d'abord défini un modèle de communication en sept couches, empilées de telle sorte que chacune s'appuie sur les services de la couche sous-jacente pour offrir à la couche supérieure un niveau de service plus élevé. Ce modèle fut standardisé sous la dénomination OSI (*Open Systems Interconnection*).

Le septième et dernier niveau de communication OSI est dédié aux applications. C'est à ce niveau qu'a été défini un système d'annuaire standardisé, d'appellation commune X.500. Ce standard spécifie un protocole de communication entre annuaires client et serveur appelé DAP (*Directory Access Protocol*).

L'inconvénient majeur des couches OSI, hormis leur complexité, est de réclamer beaucoup de ressources. Ce défaut empêchant leur support sur des équipements de faible capacité, un besoin s'est fait sentir de définir une interface plus simple. C'est ainsi qu'est né le protocole LDAP (*Lightweight Directory Access Protocol*).

Avec l'avènement des protocoles TCP/IP (ensemble de couches de communication allégé comparativement à l'OSI), LDAP a d'abord défini comment accéder à un serveur d'annuaire X.500 depuis un client supportant TCP/IP. Un serveur LDAP est défini comme une passerelle entre le monde TCP/IP du client et le monde OSI du serveur. LDAP version 2 discute des moyens d'accès à cet annuaire.

Avec la version 3, la définition LDAP franchit un pas supplémentaire en discutant de l'accès à un annuaire supportant le modèle X.500. Ce changement de langage reflète le fait que le serveur LDAP peut gérer directement l'annuaire proprement dit et se passer des couches OSI d'accès au serveur d'annuaire X.500.

LDAP version 3 permet donc de définir à la fois une passerelle d'accès à un serveur d'annuaire X.500 et un serveur d'annuaire à part entière.

1.2.4.2 Conséquences sur les standards

En tant que protocole allégé du standard X.500, LDAP a intégré des évolutions en se libérant de fonctionnalités redondantes ou jamais mises en œuvres. Il s'est aussi affranchi du standard ASN.1 (*Abstract Syntax Number One*), syntaxe complexe de représentation des données au sein du monde OSI, en spécifiant une représentation plus simple des données sous forme de chaînes de caractères. Ces évolutions impliquent une certaine indépendance de LDAP vis-à-vis du standard X.500. L'interopérabilité vis-à-vis de LDAP ne requiert donc pas de se référer au standard X.500 proprement dit, mais à l'angle sous lequel il est vu au sein de l'architecture LDAP.

Ainsi, le schéma de données du méta annuaire MAIA de l'ADAE doit se référer avant tout aux standards RFC 2252 définissant la syntaxe des attributs et RFC 2256 discutant de l'usage du schéma X.500.

Remarques :

1. le schéma de données utilise aussi des attributs de type *rfc822mailbox* et *labeledURI*, définis au sein des recommandations RFC 1274 et RFC 2079, à inclure au référentiel.
2. Le méta annuaire référence aussi des attributs de la recommandation RFC 1836 qui n'est qu'à l'état expérimental. Cette recommandation est rendue obsolète par le RFC 2294, plus stable.
3. D'autre part, un projet de référentiel a été élaboré, présentant les schémas d'annuaires interopérables des administrations, dont les résultats sont prévus pour inclusion au CCI. Ce projet référence les recommandations RFC 2247 et RFC 2798, à inclure dès à présent au CCI puisqu'elles seront mises en œuvre pour MAIA2. Les autres recommandations sont proposées pour une version ultérieure.

Plus généralement, l'ensemble des recommandations RFC 2251 à 2256 du protocole LDAPv3 est requis, dans la mesure où il est nécessaire respecter la conformité en termes de protocole d'échange, de filtres de recherche, de formats de représentation des entités du DIT (*Directory Information Tree*), etc. Pour information, le produit open source OpenLDAP est conforme à l'ensemble de ces recommandations depuis la version 2.0, sortie en août 2000.

De plus la recommandation RFC 2849 est requise pour l'alimentation de l'annuaire par fichiers au format LDIF (Cf. référentiel technique annuaire – partie 2).

1.2.4.3 Les extensions de Sécurité

Le protocole LDAP fournit des mécanismes de sécurité mis en œuvre pour garantir certains services de sécurité définis par l'ISO (ISO 7498-2) dans ses études sur la sécurité. Les éléments de sécurité pouvant être mis en œuvre par LDAPv3 sont :

- 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

L'authentification simple fournit des fonctionnalités d'authentification minimales puisque le seul champ définissant cette authentification contient uniquement un mot de passe en clair.

Cette authentification n'est donc pas recommandée pour faire de l'authentification dans les réseaux ouverts ou dans des environnements où il n'y a pas de confidentialité au niveau de la couche réseau ou de la couche transport car le mot de passe transite en clair sur le réseau et il ne peut donc pas y avoir de chiffrement ni d'authentification fiable des données.

Afin d'être exploitable, l'authentification simple doit donc être utilisée conjointement avec une connexion sécurisée contre les écoutes passives du trafic, de type TLS ou tout autre mécanisme garantissant l'intégrité et la confidentialité des données.

Sans authentification, le standard LDAP spécifie qu'il faut simplement choisir l'authentification simple et un mot de passe de longueur nulle.

Dans l'authentification LDAPv3, l'authentification simple a été améliorée avec les mécanismes SASL (RFC 2222) et DIGEST-MD5 ou avec l'ajout de la couche sécurisée TLS.

Le mécanisme SASL est une structure d'authentification pour les protocoles. Il permet donc l'authentification et l'intégrité des messages échangés et également la négociation de services de confidentialité, d'intégrité et d'authentification des données, utilisés dans le cas d'une transmission orientée connexion (TCP). L'authentification SASL permet de choisir n'importe quel mécanisme d'authentification qui peut être utilisé avec SASL.

DIGEST-MD5 fournit l'intégrité du mot de passe aussi bien que celle des données confidentielles après un échange d'authentification. La fonction MD5 fournit une empreinte du message à transmettre. DIGEST-MD5 est un mécanisme d'authentification SASL.

Le protocole TLS (présenté précédemment) 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.

Enfin, LDAPv3 offre la possibilité d'accéder à un ensemble de fonctions de sécurité qui doivent être interopérables. C'est pourquoi un minimum de ces fonctions doit être commun à toute implémentation supportant LDAPv3. Les différentes conditions de conformité d'implémentations concernent les méthodes d'authentification suivantes :

- anonymous authentication : cette méthode est généralement utilisée pour des clients qui n'ont pas l'intention de modifier des entrées ou des attributs d'entrée dont l'accès est protégé.
- DIGEST-MD5 SASL : l'accès authentifié est basé sur un mot de passe. Ce mécanisme requiert une authentification du client pour parer à des attaques passives de types écoute du trafic et à des attaques actives sur le trafic.
- TLS + authentification simple pour une session sécurisée.
- TLS + SASL.

Ces deux dernières méthodes supportent l'authentification basée sur un mot de passe et l'authentification basée sur un certificat. Elles doivent être utilisées quand l'intégrité, l'authentification et la confidentialité des données sont exigées et assurent également une protection contre les attaques actives intermédiaires (de type man-in-the-middle).

Certaines applications nécessitent que les données sauvegardées dans un annuaire LDAP soient signées. Cette signature permet de garantir l'intégrité de ces données et leur authenticité. Les spécifications en cours d'élaboration (RFC 2649) consistent à définir des extensions des fonctions de recherche et de mise à jour, afin de pouvoir manipuler des données signées.

Afin d'assurer la confidentialité et l'intégrité des entrées de l'annuaire lorsqu'elles sont accédées et manipulées, des règles d'accès (ACLs) aux données doivent être définies. LDAP, en tant que protocole d'accès aux informations d'un annuaire, requiert donc de définir un modèle de contrôle d'accès efficace pour fournir un accès autorisé aux annuaires et une interopérabilité entre eux. Le contrôle d'accès est caractérisé par les points suivants:

- L'autorisation est basée sur l'identité authentifiée du client
- La liste du contrôle d'accès (ACL) pour chaque objet est définie de la manière suivante:
 - Liste des clients ayant accès
 - Droits d'accès pour chaque client
- Les droits d'accès peuvent s'appliquer à une entrée ou sur les attributs d'une entrée

Une ACL doit permettre d'accéder à des ressources en l'associant à un sous-ensemble entier de l'annuaire, et doit supporter l'accès aux attributs d'une unique entrée. Les règles d'accès peuvent donc être appliquées à tout l'annuaire, à un sous-ensemble, à une ou plusieurs entrées particulières ne faisant pas partie d'un même sous-ensemble de l'annuaire ou aux attributs d'une entrée. Des entrées peuvent également être accédées publiquement et peuvent être lues par des clients non-authentifiés.

La description des droits d'accès à l'annuaire ne fait cependant pas partie du standard LDAPv3 initial, ce qui représente notamment un handicap pour l'administration de plusieurs annuaires d'origine différente via une interface unifiée (client LDAP) ou à la réplication entre annuaires provenant d'éditeurs différents. En effet, bien que chaque éditeur intègre néanmoins sa propre gestion des habilitations, chaque solution utilise actuellement une syntaxe propriétaire pour décrire des droits d'accès de certains objets de l'annuaire sur d'autres objets.

Les travaux menés dans le cadre de la RFC 2820 imposent le rajout au standard LDAP d'un attribut (`aci`) contenant une chaîne de caractère décrivant les droits d'accès sur l'objet dans le schéma pour toute classe d'objet de l'annuaire. La standardisation intervient dans la définition d'une syntaxe particulière à laquelle chaque éditeur devra se conformer afin de respecter le standard.

Les opérations relative à la modification des données de l'annuaire sont enregistrées dans un journal par le mécanisme d'*Audit Trail* qui gère l'historique des changements. L'*Audit Trail* permet également de sécuriser ces traces avec S/MIME en demandant à celui qui soumet l'opération devant entraîner une modification des données soit de signer directement l'opération, soit d'adresser une demande au serveur LDAP de signer le opération en son nom, en tant que client LDAP et en utilisant sa propre identité.

1.2.4.4 Standards applicables

Les recommandations relatives à la sécurité (du type certificats X.509) ne sont pas mentionnées au tableau ci-dessous. Elles sont reportées au chapitre sécurité prévu à cet effet.

STANDARD	RFC	DATE	ETAT	REMARQUES
LDAP - V3	2251	Déc- 97	Proposé	
	2252	Déc-97	Proposé	
	2253	Déc-97	Proposé	
	2254	Déc-97	Proposé	
	2255	Déc-97	Proposé	
	2256	Déc-97	Proposé	
Internet X.500	1274	Nov-91	Proposé	Attribut mail de type rfc822mailbox
X.500 URI attribut	2079	Jan-97	Proposé	Attribut site portail de type LabeledURI
Hiérarchie O/R dans le DIT X.500	2294	Mar-98	Proposé	Messagerie X.400
LDIF	2849	Jui-00	Proposé	Mise à jour LDAP par fichiers
Extensions LDAP	2798	Avril-00	Information	Classe d'objet inetOrgPerson
	2247	Janv-98	Proposé	Utilisation des noms de domaines pour les DN LDAP/X.500
Extensions de Sécurité LDAP	2649	Août-99	Expérimental	Control et schéma LDAP pour les opérations de signature
	2820	Mai-00	Informationnel	Contrôle d'accès pour LDAP
	2829	Mai-00	Proposé	Méthodes d'authentification pour LDAP
	2830	Mai-00	Proposé	Extension LDAPv3 pour TLS
	3377	Sep-02	Proposé	Spécifications Techniques LDAPv3

1.2.4.5 Candidats au référentiel Vx

STANDARD	RFC	DATE	ETAT	REMARQUES
Extensions LDAP	2927	Sept-00	Information	Extensions MIME
	2377	Sept-98	Information	Extensions pour le nommage Internet
	2307	Mars-98	Expérimental	Introduction des entités TCP/IP et Unix
	1617	Mai-94	Information	Aide à la définition d'annuaire

1.2.4.6 L'infrastructure à clé publique

1.2.4.6.1 PKI

Avec l'accroissement du nombre d'applications, de solutions techniques et d'utilisateurs faisant appel à des certificats numériques, il peut devenir nécessaire de mettre en place des outils techniques et des procédures organisationnelles afin de gérer le cycle de vie des certificats numériques à grande échelle et d'instaurer véritablement la confiance inhérente à leur utilisation. C'est précisément le rôle d'une ICP (Infrastructure de Gestion de Clés).

Les fonctionnalités offertes par une PKI via ses différentes composantes permettent d'assurer la gestion du cycle de vie d'un certificat. Une PKI s'articule généralement au minimum autour des trois composants de base suivants :

- L'Autorité de Certification (AC) qui génère et signe les certificats. L'AC est le tiers de confiance dont la signature apparaît sur le certificat. Elle est responsable du processus de certification dans sa globalité
- Une ou plusieurs Autorités d'Enregistrement (AE) qui enregistrent et valident les demandes de certificats.
- Un dépôt qui stocke les certificats et les listes de certificats révoqués (CRL : Certificate Revocation List).

Le sujet de l'ICP étant largement couvert dans le « Rapport de validation des standards et des référentiels figurant dans le cadre commun d'interopérabilité – Première version », nous nous contenterons ici d'évoquer les quelques évolutions des standards sur lesquels elle s'appuie.

1.2.4.6.2 Standards applicables

STANDARD	RFC	DATE	ETAT	REMARQUES
PKI	2510 & 2511	Mar-99	Proposé	Protocole et format de message pour une demande de création de certificat à une AC
	2559	Avr-99	Proposé	Utilisation de LDAPv2 dans une PKI
	2560	Juin-99	Proposé	OCSP
	2585	Mai-99	Proposé	Utilisation de FTP et HTTP afin de récupérer un certificat ou une CRL
	2587	Juin-99	Proposé	Schéma LDAPv2 pour une PKI
	2985	Nov-00	Information	PKCS #9 v2.0 (RSA)
	3279	Avr-02	Proposé	Algorithmes et identifiants pour le profile des certificats et des CRL
	3280	Avr-02	Proposé	Profile des certificats et des CRL
	3281	Avr-02	Proposé	Profile de certificat d'attribut pour l'autorisation

1.2.5 La qualité de service

La Qualité de Service est un aspect important de l'interconnexion de réseaux. Un référentiel de qualité de service inter administrations a d'ailleurs été élaboré à cet effet. Inclus dans la charte ADER, il a pour objets d'offrir aux administrations une méthode d'évaluation basée sur une référence commune, ainsi qu'un objectif de niveau de qualité de service de bout en bout.

L'objectif à terme est de définir plusieurs classes de service, valables pour toutes les administrations, qui devront correspondre à des besoins bien identifiés.

Une fois ces éléments établis, il sera alors question de mettre en œuvre des mécanismes propres à rendre les différentes qualités de service voulues. Pour cela, l'application de standards de l'Internet devra permettre d'offrir les fonctionnalités souhaitées, notamment en matière de services réseaux.

1.2.5.1 Les standards de la Qualité de Service

1.2.5.1.1 Principes

En matière de qualité de service Internet, deux modèles ont été proposés :

- le modèle de services intégrés (*IntServ*),
- le modèle de services différenciés (*DiffServ*).

Le modèle de services intégrés

Ce modèle repose sur le principe de réservation des ressources le long du réseau afin d'assurer la bande passante ou le délai garanti. Cette réservation s'effectue par l'utilisation d'un protocole de signalisation, dénommé RSVP (*Resource Reservation Protocol*), en préambule à la communication proprement dite.

L'émetteur soumet un paquet d'information au réseau, à des fins de repérage du chemin au sein des nœuds d'interconnexion par lesquels il passe. Ce paquet arrivant au destinataire de la communication, ce dernier répond à la requête. La réponse reprend le même chemin, déjà mémorisé par le réseau, chaque nœud d'interconnexion réservant alors les ressources requises. La communication effective peut alors commencer.

Ce modèle propose donc une qualité de service garantie dans un sens donné, pour un flux de transport donné.

Le modèle de services différenciés

Ce modèle repose sur la spécification et le contrôle du trafic réseau par classe pour permettre à certains types de trafic de prendre de l'ascendant sur d'autres. Un ensemble de règles appliquées sur les paquets permet d'attribuer une variété de comportements de transmission au sein des nœuds d'interconnexion. Ces règles sont marquées au sein des paquets IP par une série de 6 bits, appelée DSCP (*Differentiated Services Code Point*), prise dans le champ d'en-tête *Type Of Service* des paquets IPv4 ou *Traffic Class* des paquets IPv6. Elles définissent des caractéristiques quantitatives (débit, délai, taux de perte,...) et des priorités relatives.

Le traitement aux nœuds d'interconnexion est défini par un PHB (*Per Hop Behaviour*). Un petit nombre de PHB sont définis pour permettre une gestion raisonnablement fine des ressources. Un PHB décrit un niveau particulier de service en termes de bande passante, de théorie de file d'attente et de suppression de paquets. Les opérations sophistiquées de classification et de conditionnement du trafic sont généralement reportées aux frontières du réseau ou aux stations d'extrémité.

Ce modèle propose ainsi une qualité de service globale dans un sens donné, pour un type de trafic donné.

1.2.5.1.2 Les tendances

La tendance actuelle des opérateurs est d'adopter une politique de type *best effort*. Il s'agit d'adopter un traitement minimal au cœur du réseau pour atteindre les performances maximales. Cette politique permet d'utiliser des algorithmes de routage rapide, de sorte que le réseau puisse se reconfigurer de manière quasi instantanée en cas de congestion. La bande passante souscrite par un client peut être surveillée, un lien supplémentaire pouvant aisément être mis en œuvre quand la charge devient trop importante.

Le modèle de services intégrés s'accorde mal avec cette tendance. Chaque nœud d'interconnexion devant reconnaître l'identité d'un flux au sein des paquets qu'il reçoit (flux de transport), il doit traiter le contenu de ces paquets. Cette gestion, répétée en chaque nœud traversé, est pénalisante pour les performances du réseau.

D'autre part, les paquets d'un flux de données doivent être remis à un nœud destinataire prédéfini par la réservation initiale des ressources. Aussi, bien qu'une politique de reconfiguration soit possible via le protocole RSVP, cette reconfiguration ne peut pas s'effectuer rapidement en cas d'indisponibilité d'un lien.

En revanche, dans le cas du modèle de services différenciés, les nœuds d'interconnexion n'ont qu'à traiter l'en-tête des paquets IP, ce qu'ils faisaient déjà auparavant. De plus, les algorithmes de routage ne sont pas remis en cause. Cette solution s'accorde donc mieux avec la politique du *best effort*.

Ainsi, les opérateurs ont généralement abandonné le modèle *IntServ* au profit du modèle *DiffServ*. Ce qui n'empêche pas l'application des fonctionnalités RSVP, mais aux extrémités seulement. Il est à supposer que ce dernier modèle est celui retenu, à voir le référentiel déjà envisagé pour les versions ultérieures.

1.2.5.1.3 Candidats au référentiel Vx

Les standards applicables restent inchangés par rapport au référentiel prévisionnel. Il est proposé de les intégrer au référentiel courant du cadre commun d'interopérabilité lorsque leur mise en œuvre sera effective.

STANDARD	RFC	DATE	ETAT	REMARQUES
RSVP	2205	Septembre 97	Proposé	
DiffServ	2474	Décembre 98	Proposé	
	2597	Juin 99	Proposé	
	2598	Juin 99	Proposé	

1.3 INTEGRATION DES DONNEES

1.3.1 Les langages XSLT et XPath

Le langage XSLT spécifié par le W3C permet de formater les documents XML, et d'effectuer des transformations sur ces documents. Une *transformation* est une description de règles pour transformer un *arbre source* (un ou plusieurs documents) en un *arbre résultat*. Une règle associe un *filtre* (si...conditions dans l'arbre source) à un *modèle* (alors...dans l'arbre résultat). Pour accéder aux données XML le développeur dispose d'expressions formalisées en langage XPath spécifié également par le W3C.

1.3.1.1 Tendances

Ce langage étant destiné originellement à des non informaticiens, il a été par la suite largement adopté par la communauté des développeurs. De ce fait des limitations sont apparues dans le cadre d'utilisations professionnelles. Il a donc été décidé de définir les évolutions nécessaires dans une version 2.0. Cette nouvelle version est publiée par le W3C afin de fournir à la communauté des utilisateurs de XSLT une première vue de la spécification modifiée du langage et d'obtenir des commentaires... Bien que des implémentations de prototypes soient encouragées, les utilisateurs et les vendeurs sont avertis que cette version de travail ne peut pas être considérée comme une spécification stable.

Les principales évolutions d'XSLT 2.0 portent sur la gestion :

- des collections,
- des tris (enrichissements),
- des fonctions utilisateur,
- La possibilité de produire des arbres résultats multiples,
- La possibilité de sortie en XHTML.

Avec XPath 2.0 les utilisateurs peuvent accéder au typage simple des données (entiers, chaînes, flottants, dates, etc.). En outre, un certain nombre de fonctions et d'opérateurs sont donnés pour traiter et construire ces différents types de données. Et enfin il est possible d'utiliser des collections ainsi que des opérateurs conditionnels dans les expressions.

1.3.1.2 Candidats au référentiel Vx

Les standards applicables restent inchangés par rapport au référentiel prévisionnel. Il est proposé d'intégrer ces nouvelles normes au référentiel Vx du cadre commun d'interopérabilité.

Composant	Standard	RFC	Date / Version	Etat du standard	Commentaires
Outils de traitement et de présentation des données	XSL (Extensible Stylesheet Language) XSLT 2.0 XPATH 2.0	http://www.w3.org/TR/xslt20/ http://www.w3.org/TR/xpath20/	nov-02	Draft	A suivre pour prise en compte ultérieure (lorsque le standard sera industriellement reconnu)

1.3.2 La sécurité XML

XML est LE format standard d'échange de données. Il joue un rôle à tous les niveaux de l'architecture, depuis les appareils de communication (dans une approche multicanal) jusqu'aux applications existantes, en passant par le portail.

L'essor de la technologie des Web Services (s'appuyant principalement sur XML, SOAP, WSDL et UDDI, cf. chapitre 1.5 « Les architectures applicatives » page 47) est un pas énorme dans la capacité à intégrer des processus applicatifs de manière beaucoup plus transparente, tant en terme de développement technique qu'en terme de localisation des applications. Il existe aujourd'hui des sites en production utilisant de manière plus ou moins étendues les Web Services, mais il faut encore à l'heure actuelle peser le pour et le contre au cas par cas, les travaux de standardisation sur certains aspects étant encore en cours.

Ainsi, émergents au rythme soutenu des nouvelles propositions de ses principaux contributeurs, les Web Services, nouveau standard d'interopérabilité entre les applications, apportent leur lot de préoccupations, notamment en matière de sécurité.

Tout d'abord, leur encapsulation fréquente au sein du protocole HTTP, bien que judicieuse pour des besoins d'échange, rendent inefficaces les solutions de protections habituelles. De nouveaux coupe-feu analysant les messages SOAP voient progressivement le jour afin d'y remédier.

De plus, l'absence volontaire de fonctions de sécurité au niveau de SOAP freinait jusqu'à présent leur déploiement hors du contexte fermé de l'entreprise malgré l'émergence d'initiatives telles que la standardisation des fonctions de signature (XML-Signature) et chiffrement (XML- Encryption) de documents XML.

La diffusion mi-2002 de propositions majeures (ayant pour vocation de devenir des standards) comble ce vide avec notamment WS-Security (cf. chapitre 1.5 « Les architectures applicatives » page 47), qui apporte un support global de l'intégrité, de la confidentialité et de l'authentification des messages, et SAML, qui définit un langage commun d'interopérabilité permettant de décrire et partager des informations liées à l'authentification et l'autorisation afin de faciliter la mise en place de fonctionnalités SSO et de permettre la délégation de droits. D'autres propositions émergentes, telles que XKMS ou XACML viennent compléter les manques en matière de sécurité.

1.3.2.1 XML-Signature

XML Signature est un protocole développé par le W3C qui décrit la signature d'un contenu numérique dans le cadre de transactions XML. En fait le standard définit un schéma afin de récupérer le résultat d'une signature numérique d'un donnée arbitraire (souvent du XML) et, à l'instar des signatures numériques non-orientées XML (comme PKCS), les signatures XML apporte l'authentification, l'intégrité des données et le support de la non-répudiation des données signées.

Cependant, contrairement aux standards de signature non-orientés XML, XML Signature a été conçu pour prendre en compte à la fois les avantages de l'Internet et de XML. Ainsi une fonctionnalité fondamentale de XML Signature tient dans sa capacité à signer uniquement une partie spécifique d'un arbre XML plutôt que de signer le document complet. Cela est pertinent lorsqu'un simple document unique a une longue histoire dans laquelle les différents composants sont créés à des moments différents et par des parties distinctes, chacune signant ses propres éléments. Cette flexibilité est aussi critique dans des situations où il est important d'assurer l'intégrité de certaines parties du document XML tout en laissant la possibilité à d'autres parties de changer.

Une signature XML peut également s'appliquer à plusieurs type de ressource en même temps. Par exemple, une seule signature XML peut couvrir des données HTML, une image JPEG, de données codées XML ainsi qu'une partie spécifique d'un fichier XML.

La validation de la signature requiert que l'objet de donnée qui a été signé soit accessible. La signature XML indique donc généralement l'emplacement de l'objet original signé. Cette référence peut :

- Etre spécifiée par un URI (Uniform Resource Identifier) au sein de la signature XML ;
- Résider au sein de la même ressource que la signature XML ;
- Être encapsulée au sein de la signature XML ;
- Avoir sa signature XML encapsulée dans elle même

1.3.2.2 XML-Encryption

XML Encryption est un protocole développé par le W3C qui décrit le principe de chiffrement d'un contenu numérique. Le standard XML Encryption inclut des protocoles pour chiffrer les sections des documents XML. XML Encryption permet un chiffrement de bout en bout car le contenu du message est chiffré alors que le chiffrement effectué au niveau session assure uniquement la confidentialité des données entre deux serveurs.

1.3.2.3 XKMS

XKMS (XML Key Manipulation Service) dynamise le framework Web services en permettant aux développeurs de sécuriser les échanges en s'appuyant sur une PKI.

XKMS est une spécification fondamentale pour la mise en œuvre de Web Services sécurisés, en leur permettant d'enregistrer et de gérer les clés de cryptographie utilisées pour la signature et le chiffrement.

L'initiative XKMS rend la PKI largement accessible en permettant aux développeurs de compter sur des Web Services de confiance orientés XML afin de réaliser les fonctions de la PKI. Ces Web Services de confiance résident sur l'Internet et peuvent être accédés par n'importe quelle application. Au lieu de coder des fonctions PKI complexes, les développeurs utilisent simplement XML afin de se rattacher à un service de confiance qui réalise la plupart des tâches complexes de gestion des clés. Ainsi, en déléguant la complexité de la PKI à ces services de confiance, les développeurs peuvent se concentrer sur le cœur de l'application.

En utilisant XKMS, les services de gestion des clés peuvent être plus déployés rapidement et intégrés dans une plus grande variété d'applications. Autre point important, le faible overhead induit par les applications XKMS permet de porter le support PKI sur des équipements disposant de peu de mémoire.

Les bénéfices de XKMS sont donc nombreux, tels que :

- La facilité d'utilisation, du fait de l'utilisation d'une « boîte à outils » XML standardisé plutôt que des boîtes à outils PKI et des plug-ins propriétaires ;
- La rapidité de déploiement des applications ayant besoin d'établir la confiance, du fait du déplacement de la complexité de développement côté serveur ;
- L'ouverture, du fait de l'indépendance de XKMS par rapport aux éditeurs, aux plate-formes et au protocole de transport ;
- La pérennité, du fait que les développements futurs en matière de PKI n'impacteront que les composants situés côté serveur.

1.3.2.4 XACML

XACML (eXtensible Access Control Markup Language) est une spécification de l'OASIS qui est utilisée conjointement avec SAML (Cf. paragraphe suivant) dans le but de standardiser les décisions de contrôle d'accès aux documents XML. En s'appuyant sur des règles ou une politique définie par le propriétaire du document, XACML reçoit une requête SAML et détermine si l'accès à la ressource XML doit être accordé totalement, partiellement ou non.

Contrairement à XML Encryption, les informations de contrôle d'accès sont situées à endroit physiquement séparé du document XML, endroit auquel il est fait référence lors de la requête. XPointers et XPath sont en effet définis au sein des tags XML et indiquent à l'analyseur syntaxique XML de vérifier les politiques XACML et l'endroit où les trouver.

Une fois que la politique est évaluée et qu'elle retourne une valeur vrai ou fausse pour indiquer si l'accès est autorisé ou non, une déclaration d'autorisation SAML est retournée qui est alors traitée en conséquence par l'entité appelante.

1.3.2.5 SAML

Security Assertion Markup Language est développé par le W3C et est un protocole de déclaration de données d'authentification et d'autorisation. La nouvelle spécification SAML 1.0 est issue de la fusion de deux anciens travaux concurrents S2ML et AUthML. L'ensemble de SAML 1.0 a été dévoilé en Février 2002 et les spécifications ont été présentées à l'OASIS (Organization for the Advancement of Structured Information Standards) en Mars 2002 en vue d'une standardisation par le comité technique des services de sécurité de l'OASIS.

Les données utilisateur d'authentification et d'autorisation, les profils et les préférences sont transmis d'un fournisseur de services à d'autres choisis par l'utilisateur au cours de la session.

SAML permet une conception ouverte et interopérable pour des services de type Web-SSO. L'utilisation de SAML pour le SSO permet à un utilisateur de s'authentifier dans un domaine et d'utiliser les ressources dans un autre domaine sans qu'il ait à s'authentifier de nouveau.

L'idée de services de SSO n'est pas nouvelle et des solutions propriétaires existent depuis des années mais elles offrent peut d'interopérabilité. SAML, par contre, constitue une approche ouverte et pleinement interopérable afin d'échanger des informations de sécurité dans le cadre d'un SSO.

1.3.2.6 Standards applicables

Composant	Standard	RFC	Date / Version	Etat du standard	Commentaires
Sécurité XML	XML Signature XMLDSIG	N/A	février-02	Recommandation W3C	XML Signature Syntax and Processing- http://www.w3.org/TR/2002/REC-xmlsig-core-20020212/
		RFC 2807	juillet-00	Informationnel	XML Signature Requirements
		RFC 3275	mars-02	Proposé	XML Signature Syntax and Processing
	XML Encryption XMLENC	N/A	mars-02	Draft W3C	XML Encryption Requirements - http://www.w3.org/TR/xml-encryption-req
		N/A	décembre-02	Draft W3C	XML Encryption Syntax and Processing - http://www.w3.org/TR/xml-encryption-req
		N/A	décembre-02	Draft W3C	Decryption Transform for XML Signature - http://www.w3.org/TR/xmlenc-decrypt

1.3.2.7 Candidats au référentiel Vx

Composant	Standard	RFC	Date / Version	Etat du standard	Commentaires
Sécurité XML	XKMS	N/A	mars-02	Document de travail W3C	Spécifications XKMS 2.0 - http://www.w3.org/TR/xkms2/
		N/A	mars-02	Document de travail W3C	Exigences XKMS - http://www.w3.org/TR/xkms2-req
	XACML	N/A	déc-02	Spécifications OASIS	Spécifications XACML - http://www.oasis-open.org/committees/xacml/repository/cs-xacml-specification-01.pdf
		N/A	mai-02	Spécifications	Définition du protocole http://www.oasis-open.org/committees/security/docs/cs-sstc-core-01.pdf
	SAML	N/A	mai-02	Spécifications	Règles d'interfaçage avec SAML http://www.oasis-open.org/committees/security/docs/cs-sstc-bindings-01.pdf
		N/A	mai-02	Spécifications	Considérations relatives à la sécurité et à la protection de la vie privée http://www.oasis-open.org/committees/security/docs/cs-sstc-sec-consider-01.pdf
		N/A	mai-02	Spécifications	Programme de conformité à SAML http://www.oasis-open.org/committees/security/docs/cs-sstc-conform-01.pdf
		N/A	mai-02	Spécifications	

1.3.3 Le langage UML

Le langage UML (Unified Modeling Language) est un langage graphique et textuel qui permet de représenter et de modéliser des données et des processus, des interactions entre systèmes ou composants, et d'organiser les données, les composants ou les systèmes dans différents types de hiérarchie (taxinomie, composition, package, composant, etc.).

Le langage UML est objet, c'est à dire qu'il permet d'une part de représenter dans une même entité (la classe) les aspects structurels et comportementales d'un concept et d'autre part de pouvoir décrire une taxinomie, c'est à dire de hiérarchiser les concepts du plus général au plus spécifique, ces derniers héritant des caractéristiques des plus généraux. La représentation objet permet donc de mieux décrire aussi bien les objets du monde réel que ceux des systèmes informatique car elle permet de réaliser de manière plus cohérente et contrôlée les futures corrections ou évolutions.

En effet le concept de classe permet de faire évoluer le système en définissant d'autres sous-classes d'une classe, sans que cet ajout perturbe les autres classes déjà définies ; les modifications apportées à une classe se répercutent sur toutes ses sous-classes éventuelles et sont en principe circonscrites à cette classe, l'aspect « donnée » et « comportement » étant défini dans cette classe et non de manière séparée comme dans les autres types de langage.

Le langage UML dans sa version 1.1 fut adopté en novembre 1997 par l'Object Management Group (OMG) comme le standard de modélisation objet. Il est issu initialement de trois méthodes OOA/OOD de G. Booch, OMT de J. Rumbaugh et OOSE de I. Jacobson et est le résultat du travail et des recommandations de personnes et d'entreprises réparties dans le monde entier.

Ce langage est largement répandu dans tous les secteurs (public, industrie, militaire, finance, assurance, santé, etc.) pour la représentation, la spécification et la réalisation de systèmes (logiciel ou organisation) et est supporté par un nombre important d'outils. Quasiment tous les ateliers d'analyse et de conception UML

du marché proposent des générateurs de code vers les langages C++, Java, etc. d'autres montrent en même temps le code Java associé à certains éléments du modèles (les classes).

UML définit 12 types de diagrammes, divisé en 3 catégories : 4 pour représenter la structure statique de l'application, 5 pour représenter les différents aspects du comportement dynamique et 3 pour organiser les modules de l'application :

- Diagramme de structure : diagramme de classe, objet, composant, et déploiement
- Diagramme de comportement : diagramme de use-case, de séquence, d'activité, de collaboration, d'état.
- Diagramme d'organisation : diagramme de package, de sous-système, de modèle.

La version actuelle est la version 1.4. et date de septembre 2001.

Plusieurs raisons conduisent à préconiser le langage UML dans le cadre de l'interopérabilité **pour la version v2.**

- 1) La première raison de mettre le langage UML en version v2 est qu'il est opérationnel et que c'est déjà un standard international.
- 2) Il est nécessaire de représenter et de décrire dans un langage « semi-formel » les concepts en jeu dans les interactions entre systèmes, à des fins de documentation et de communication avec les différents acteurs intervenants dans la réalisation d'un système. Ce langage doit être le même entre les différents acteurs pour éviter toute ambiguïté.
- 3) La représentation graphique associée à une organisation en plusieurs points de vue ou par thème permet de visualiser de manière synthétique les concepts selon différents axes (statique ou dynamique, selon le cycle de réalisation – analyse, conception, réalisation, ... - par domaine d'intérêt, etc.)
- 4) La représentation objet permet d'analyser et de maîtriser la complexité des systèmes par l'organisation hiérarchique (taxinomie, composition, association, package, composants) des concepts. Cette organisation permet aussi de définir et d'allouer un périmètre fonctionnel, organisationnel et physique aux différents acteurs du système
- 5) Ce langage est largement répandu et utilisé dans la réalisation de systèmes informatiques, de représentation de concepts, de tout type (humain, mécanique, informatique, ...) de processus et activités. Il n'existe à ce jour pas de concurrent sérieux dans ce domaine
- 6) Il permet de représenter les concepts mis en œuvre dans le cadre de l'interopérabilité :
 - a) les processus d'échanges d'information entre les systèmes ou les organismes par les diagrammes d'activité et dans une spécification plus détaillée par les diagrammes de séquences et les diagrammes d'état
 - b) les acteurs et les scénarios d'utilisation par les diagrammes de cas d'utilisation. Un document textuel est associé à chaque cas d'utilisation pour décrire un ou plusieurs scénarios d'utilisation : le déclenchement du cas d'utilisation puis l'enchaînement des actions effectuées par les différents acteurs intervenant dans le cas d'utilisation, les échanges d'information, les cas d'erreurs et les traitements associés
 - c) les données échangées ou les référentiels communs par les diagrammes de classes, d'objets
 - d) les modules, systèmes ou sous-systèmes, composants matériels par les diagrammes de package, de composants ou de déploiement, pour décrire l'architecture logique et physique et indiquer les interfaces disponibles des systèmes
- 7) La plupart des outils d'analyse UML permettent de générer l'analyse au format XML. Pour cela la plupart utilisent le format standard de l'OMG, XML Metadata Interchange (XMI 1.2). Le but de ce format est faciliter l'échange de méta-données entre les outils de modélisation (basé sur UML) et entre les outils et les référentiels de données dans des environnements distribués hétérogènes. XMI intègre 3 formats standards :
 - a) XML, eXtensible Markup Language, un standard W3C

- b) UML, Unified Modeling Language, un standard OMG
- c) MOF, Meta Object Facility, un standard OMG

XMI est applicable sur de nombreux types d'objets : les objets d'analyse et de conception (UML), logiciels (Java, C++), composants logiciels (EJB, IDL, CORBA) et de bases de données (CWM) et permet aux développeurs de partager des modèles objets dans des environnements distribués via internet.

La version actuelle est la version 1.2. La future version 2.0 supportera la notion de schéma XML.

1.3.3.1 Standards applicables

Composant	Standard	RFC	Date / Version	Etat du standard	Commentaires
Language de description et de modélisation des données	UML	http://www.omg.org/uml/	sept. 2001 / v1.4	ouvert, très utilisé, standard OMG	UML (Unified Modeling Language) de l'OMG (Object management Group). Ce langage permet de modéliser les processus et les données

1.3.4 La méthodologie UN/CEFACT Modeling Methodology (UMM)

UMM est une méthode, indépendante de la technologie et de l'implémentation, pour modéliser les processus commerciaux et permettre le développement de la nouvelle et actuelle génération d'EDI pour le commerce électronique. Cette méthode s'appuie sur le langage UML et part de la méthode Unified Process développée par Rational Corporation (RUP) appliquée à la modélisation des processus commerciaux.

Cette méthode s'appuie sur le Business Operations View du standard ISO/IEC 14662 et permet de définir n'importe quel scénario open-edi défini par ce standard.

UMM fournit une extension du méta-modèle UML grâce à des stéréotypes UML spécifiques au domaine commercial ainsi que des descriptions de processus, de concepts et des patterns pour aider les experts et les analystes du domaine dans la modélisation.

Nous préconisons de laisser cette méthodologie en Vx, car elle est récente et peu reconnue et aussi parce que les points que cette méthodologie adresse pourraient être utiles dans le cadre de l'interopérabilité.

1.4 FORMATS DES DONNEES NUMERIQUES

1.4.1 Jeux de caractères et alphabets

Le jeu de caractères utilisé pour la fourniture de données textuelles est un des éléments qui permettent l'interopérabilité. La recommandation du CCI est l'utilisation de la norme Unicode. Cette norme, choisie notamment pour XML, respecte la norme ISO 10646-1 - Universal Multiple-Octet Coded Character Set (UCS), dans sa version restreinte au codage sur deux caractères, mais intègre des contraintes supplémentaires. La norme ISO permet aussi un codage sur quatre caractères, non repris par Unicode.

Le codage Unicode est effectué sur deux octets. Comme les 256 premières valeurs de la norme ISO 10646-1 correspondent à la norme ISO 8859-1 latin 1, certains codages se réclament à tort d'Unicode alors qu'ils sont simplement à la norme ISO 8859-1 latin 1. D'autres codages utilisent des caractères d'échappement pour coder les caractères sur un nombre variable de caractères, ce qui est un écart par rapport à la norme.

Les données transmises doivent comporter l'indication de l'utilisation du jeu de caractères Unicode.

1.4.2 Formats de documents

1.4.2.1 TXT

Les fichiers textes sont pérennes car très simples, mais ils induisent une perte d'information sensible. D'autre part le codage des fins de lignes n'est pas standardisé. Il est conseillé de les migrer vers XML.

1.4.2.2 XML

Le choix de XML comme format d'échange de données textuelles et multimédia est recommandé par le CCI. XML (Extensible Mark-Up Language) est basé sur SGML. Le langage XML a été conçu et promu par l'association W3C (World Wide Web Consortium), l'organisme de régulation d'Internet. L'utilisation de la norme XML n'implique pas de versement de droits d'auteur. XML est abordé en détail au chapitre « Intégration des données » du CCI.

À titre d'exemple, les différents composants de la suite bureautique OpenOffice.org stockent leurs données au format XML.

1.4.2.3 SGML

SGML (Structured General Mark-Up Language) est un langage de description de documents défini par la norme ISO 8879 : 1986. Il est fortement utilisé pour certains secteurs de la documentation industrielle, mais son utilisation n'est plus en croissance. La recommandation du CCI pour les administrations est de migrer les documents SGML vers XML pour une meilleure interopérabilité.

1.4.2.4 HTML

HTML (Hyper Text Mark-up Language) est une implémentation simplifiée du langage SGML. Il est recommandé :

- de faire figurer le numéro de la version utilisée, ainsi que les feuilles de style utilisées,
- de vérifier la conformité des pages HTML produites à l'aide de l'outil de validation fourni sur le site du W3C.

1.4.2.5 RTF

RTF (ou Rich Text Format) est un format propriétaire de Microsoft, destiné à l'échange de documents. C'est un format très fréquent qui peut être utilisé pour l'échange de données. Il est cependant conseillé de faire migrer, lorsque c'est possible, ces données vers XML. Il devrait être possible, pour ce faire, de tirer parti des fonctions XML annoncées dans MS Office 11.

1.4.2.6 PDF

Le format PDF, ou Portable Document Format, est un format propriétaire de la société Adobe, lié au logiciel Acrobat. Il permet la restitution d'une version imprimée à l'identique, quelque soit le système d'exploitation utilisé. Son usage est très répandu, notamment dans les administrations.

Adobe diffuse actuellement gratuitement le logiciel de lecture Acrobat Reader, sous réserve de l'acceptation de la licence. La gratuité d'Acrobat Reader n'est cependant pas garantie dans le temps.

1.4.2.7 XHTML

XHTML est une recommandation du World Wide Web Consortium (W3C), définie le 26/01/2000 et mise à jour le 01/08/2002. Elle est basée sur XML et définit une syntaxe proche de HTML 4.0 mais plus contrainte.

Un document XHTML est décrit par une DTD. Trois types de DTD sont définis :

- *strict*,
- *transitional* : la DTD autorise les balises de présentation (*presentational tag*),
- *frameset* : en plus de ce que permet « *transitional* », la DTD autorise les *frames*.

L'objectif du W3C est de faire migrer les documents HTML vers XHTML, qui est mieux à même de représenter des informations complexes.

L'utilisation de cette norme étant encore faible, elle est proposée pour une version ultérieure du CCI.

1.4.2.8 OASIS Open Office XML Format

OASIS a constitué un groupe de travail pour normaliser un format d'échange de documents basé sur XML, en prenant comme base le format utilisé par OpenOffice.org.

Une fois défini, ce format peut constituer un cadre de référence pour l'échange de documents.

Compte tenu de son développement en cours, cette norme est proposée pour une version ultérieure du CCI.

1.4.2.9 Microsoft Office v11 XML Format

Microsoft annonce pour la version 11 d'Office, une intégration forte de XML. Les composants d'Office pourront lire et produire au format XML. La disponibilité des spécifications d'interface d'Office 11 est un pré-requis pour la prise en compte dans une version ultérieure du CCI.

1.4.2.10 PDF/A

NPES (The Association for Suppliers of Printing, Publishing and Converting Technologies) et AIIM International (Association for Information and Image Management, International) se sont associés pour définir un format d'archivage pérenne, nommé PDF/A et basé sur le format PDF d'Adobe.

L'objectif du projet est de définir un format adapté à une conservation à très long terme, notamment pour les bibliothèques, les administrations ainsi que tous les organismes amenés à exploiter un document plus d'une centaine d'années après sa création. Une fois défini, ce format sera proposé à l'ISO.

Compte tenu de son développement en cours, cette norme est proposée pour une version ultérieure du CCI.

1.4.2.11 XForms

XForms est une recommandation candidate du World Wide Web Consortium, définie le 20/11/2002. Elle est basée sur XML et permet la réalisation de formulaires. XForms gère séparément la présentation et le contenu. XForms permet le typage des données à saisir. Cette norme n'est pas un nouveau type de document, mais est conçue pour être intégrée dans des langages comme XHTML ou SVG.

Ce projet de norme est proposé pour une version ultérieure du CCI.

1.4.2.12 Candidats au référentiel Vx

Composant	Standard	RFC	Etat du standard	Commentaires
Formats de documents	XHTML		A prendre en compte dans une version ultérieure du CCI	XHTML est une recommandation du World Wide Web Consortium, définie le 26/01/2000 et mise à jour le 01/08/2002. Elle est basée sur XML et définit une syntaxe proche de HTML 4.0 mais plus contrainte.
	OASIS Open Office XML Format	http://www.oasis-open.org/committees/office	A prendre en compte dans une version ultérieure du CCI	OASIS a constitué un groupe de travail pour normaliser un format d'échange de documents basé sur XML, en prenant comme base le format utilisé par OpenOffice.org.
	Microsoft Office v11 XML Format	http://www.microsoft.com/office/developer/prview/XML.asp	A prendre en compte dans une version ultérieure du CCI	Microsoft annonce pour la version 11 d'Office, une intégration forte de XML. Les composants d'Office pourront lire et produire au format XML. La disponibilité des spécifications d'interface d'Office 11 est un pré-requis pour la prise en compte dans une version ultérieure du CCI.
	PDF/A	http://www.aiim.org/pdf_a	A prendre en compte dans une version ultérieure du CCI	NPES (The Association for Suppliers of Printing, Publishing and Converting Technologies) et AIIM International (Association for Information and Image Management, International) se sont associés pour définir un format d'archivage pérenne, nommé PDF/A et basé sur le format PDF d'Adobe.
	XForms	http://www.w3.org/TR/xforms Candidate Recommendation 20/11/2002	A prendre en compte dans une version ultérieure du CCI	XForms est une recommandation candidate du World Wide Web Consortium, définie le 20/11/2002. Elle est basée sur XML et permet la réalisation de formulaires. XForms gère séparément la présentation et le contenu. XForms permet le typage des données à saisir. Cette norme n'est pas un nouveau type de document, mais est conçue pour être intégrée dans des langages comme XHTML ou SVG.
Flux de données audio	Ogg Vorbis	http://www.vorbis.com http://vorbis.music.free.fr v1.0	A prendre en compte dans une version ultérieure du CCI	Ogg Vorbis est une technologie d'encodage, de lecture et de diffusion audio, distribuée en logiciel libre, sous licence GPL. Ogg Vorbis a pour objectif de remplacer le format MP3.
Echange de données audiovisuelles	AAF	http://www.aafassociation.org	A prendre en compte dans une version ultérieure du CCI	AAF (Advanced Authoring Format/ Format d'édition avancé), a été développé par Avid et est proposé en format logiciel libre depuis 2000. AAF permet l'échange de données multimédias composites entre producteurs multimédia.

	MPEG-4 part 10 / H.26L	Cette norme, en cours de définition, est proposée pour une version ultérieure du CCI.	ISO/MPEG et l'UIT élaborent actuellement MPEG-4 part 10 / H.26L, avec l'objectif d'une norme ne comprenant pas de versement de redevances (<i>royalty-free</i>).
--	------------------------	---	--

1.4.3 Échange d'information graphique/images fixes

1.4.3.1 TIFF (UIT T4)

TIFF (Tag Image File Format) Groupe IV est une norme de l'Union Internationale des Télécommunications (UIT). Ce format est très répandu grâce à son exploitation par les télécopieurs et par les scanners. Il utilise des types de compression permettant de garantir la qualité et l'absence de perte. Son utilisation est possible.

1.4.3.2 PNG

Le format PNG (Portable Network Graphics) concerne les images fixes, à l'exclusion des images animées. Il vise à remplacer le format propriétaire GIF pour la compression sans pertes. Ce format est promu par l'association W3C. Son utilisation est recommandée.

1.4.3.3 GIF

GIF (Graphic Interchange Format) est un format très répandu. Ce format étant propriétaire, il y a lieu de veiller à migrer dès que possible les fichiers GIF en fichiers PNG.

1.4.3.4 JPEG

L'utilisation de JPEG (Joint Photographic Experts Group) est recommandée. Cette norme, définie par l'ISO, est très utilisée pour la photographie numérique. Elle permet un haut niveau de compression (de l'ordre de 1/40). La contrepartie est une perte d'information.

Une nouvelle norme, JPEG2000, est en cours de finalisation par le groupe de travail ISO/IECJTC 1/SC29. Elle permet d'adapter plus finement la qualité de l'image restituée à la bande passante disponible.

1.4.3.5 SVG

SVG 1.0 (Scalable Vector Graphic) est une norme du World Wide Web Consortium, définie le 04/09/2001. Elle est basée sur XML et permet la description d'objets graphiques vectoriels en deux dimensions. Elle permet l'interactivité, le scripting et l'animation.

Compte tenu de sa relativement faible diffusion, cette norme est proposée pour une version ultérieure du CCI.

1.4.4 Flux audiovisuels

1.4.4.1 MP3

MP3, abrégé de MPEG-1 Layer III Audio, est une norme de compression du son stéréophonique, devenue la référence dans le domaine de l'échange de fichiers musicaux. Les algorithmes utilisés prennent en compte la perception du son par l'oreille humaine pour obtenir un fort taux de compression avec une différence de qualité d'audition minimale.

L'utilisation de MP3 est recommandée. Cette norme intègre cependant des algorithmes brevetés, commercialisés par un groupe de revente (*patent pool*).

1.4.4.2 WAV

WAV (RIFF WAVE). À l'origine, format de fichier sonore de Microsoft Windows, il est maintenant élargi à d'autres plates-formes. Le son est stéréophonique, sans perte d'information.

1.4.4.3 MPEG-2

L'utilisation de MPEG-2 (Moving Picture Expert Group) est recommandée. Cette norme de compression pour les images animées est d'un usage très courant et fonctionne sur toutes les plates-formes.

Il faut noter que MPEG-2 intègre des algorithmes brevetés, commercialisés par un groupe de revente commun aux détenteurs de droits (*patent pool*).

1.4.4.4 MPEG-4

MPEG-4 est une norme de compression pour les images animées, définie par le Moving Picture Expert Group de l'ISO. Le dernier niveau du standard est aussi nommé H264 par l'UIT. MPEG-4 permet de gérer des flux pour l'accès à travers internet et la visioconférence, avec des débits réduits. Il faut noter que cette norme intègre des algorithmes brevetés et que les dix-huit sociétés détentrices de brevet sont encore en pourparlers pour constituer un groupe de revente commun (*patent pool*), ce qui freine sa diffusion.

DivX, parfois assimilé à tort à MPEG-4, est en fait basé sur MPEG-4 Visual pour l'image et MP3 pour le son.

1.4.4.5 DV

DV (Digital Video cassette) est un format d'acquisition vidéo défini par un consortium de sociétés. C'est le format de la vidéo numérique grand public ainsi que d'une partie des professionnels de l'audiovisuel. Compte tenu de sa diffusion, l'utilisation de ce format par les administrations est possible.

1.4.4.6 Ogg Vorbis

Ogg Vorbis est une technologie d'encodage, de lecture et de diffusion audio, distribuée en logiciel libre, sous licence GPL. L'objectif de ses créateurs est de fournir une alternative au format MP3 qui ne nécessite pas le versement d'une redevance pour la réalisation de logiciels d'encodage.

Compte tenu de son origine récente et de sa faible diffusion, cette norme est proposée pour une version ultérieure du CCI.

1.4.4.7 AAF

AAF (Advanced Authoring Format/ Format d'édition avancé), a été développé par Avid et est proposé en format logiciel libre depuis 2000. AAF permet l'échange de données multimédias composites entre producteurs multimédia. C'est un format de transport qui permet d'associer à un document audiovisuel les informations issues de son processus de création (indications de tournage, transcription des dialogues, ...) ou nécessaires à sa diffusion (sous-titres, ...).

Compte tenu de sa diffusion encore faible, ce format est proposé pour une version ultérieure du CCI.

1.4.4.8 MPEG-4 Part 10/ H26L

ISO/MPEG et l'UIT élaborent actuellement MPEG-4 part 10 / H.26L, avec l'objectif d'une norme ne comprenant pas de versement de redevances (*royalty-free*).

Cette norme, en cours de définition, est proposée pour une version ultérieure du CCI.

1.4.4.9 Candidats au référentiel Vx

Composant	Standard	RFC	Etat du standard	Commentaires
Flux de données audio	Ogg Vorbis	http://www.vorbis.com http://vorbismusic.free.fr v1.0	A prendre en compte dans une version ultérieure du CCI	Ogg Vorbis est une technologie d'encodage, de lecture et de diffusion audio, distribuée en logiciel libre, sous licence GPL. Ogg Vorbis a pour objectif de remplacer le format MP3.
Echange de données audiovisuelles	AAF	http://www.aafassociation.org	A prendre en compte dans une version ultérieure du CCI	AAF (Advanced Authoring Format/ Format d'édition avancé), a été développé par Avid et est proposé en format logiciel libre depuis 2000. AAF permet l'échange de données multimédias composites entre producteurs multimédia.
	MPEG-4 part 10 / H.26L		Cette norme, en cours de définition, est proposée pour une version ultérieure du CCI.	ISO/MPEG et l'UIT élaborent actuellement MPEG-4 part 10 / H.26L, avec l'objectif d'une norme ne comprenant pas de versement de redevances (<i>royalty-free</i>).

1.4.5 Échange de bases de données

1.4.5.1 XML

Le CCI V2 recommande d'utiliser XML pour les échanges de bases de données.

1.4.5.2 CSV (texte plat)

Le format CSV (Comma Separated Values) est un format d'échange de bases de données. Le contenu de la base à exporter est mis sous la forme d'un texte "à plat" doté de séparateurs (virgule de séparation). L'utilisation de ce format par les administrations est possible, cependant l'utilisation préférentielle de XML est recommandée.

1.4.6 Plans

1.4.6.1 CGM

Le format CGM (Computer Graphics Metafile) est une norme pour la mémorisation et l'échange de données graphiques à deux dimensions. Son utilisation est recommandée.

1.4.6.2 STEP

STEP (Standard for Exchange of Product Data) est une norme pour l'échange de nomenclatures de produits industriels. Cette norme est utilisée par certains secteurs industriels. Son utilisation est recommandée pour les administrations amenées à échanger ce type de données.

1.4.6.3 DXF

DXF est un format propriétaire utilisé par le logiciel Autocad. L'utilisation de ce format par les administrations est possible.

1.5 LES ARCHITECTURES APPLICATIVES

Pour plus d'informations détaillées sur les architectures applicatives et sur les concepts utilisés ici, se reporter à l'étude analytique en annexe 6 du CCI.

1.5.1 Les Services Web

Les services Web sont une technologie permettant à des applications de dialoguer à distance via internet et ceci indépendamment des plates-formes et des langages sur lesquelles elles reposent. Pour ce faire, les services Web s'appuient sur un ensemble de protocoles standardisant les modes d'invocation mutuels de composants applicatifs.

En d'autres termes, les services Web permettent à des applications externes de localiser, d'exécuter d'autres applications résidants sur un réseau local ou public et, par la même occasion, échanger l'information via de simples messages basés sur XML.

Reposant sur le langage de balisage XML, le protocole SOAP (Simple Object Access Protocol) définit la structure des messages échangés par les applications via Internet.

Un service Web doit préalablement être décrit à l'aide du langage de description WSDL (Web Service Description Language).

Enfin, il peut être enregistré dans le registre UDDI (the Universal Description, and Discovery Integration). Il s'agit d'un annuaire mondial basé sur le Web qui décrit les informations relatives aux services (nom, société, description, localisation, etc...). Son objectif étant a terme d'automatiser les procédures de recherche et de découverte des services par les clients.

L'essor de cette technologie est un pas énorme dans la capacité à intégrer des processus applicatifs de manière beaucoup plus transparente, tant en terme de développement technique qu'en terme de localisation des applications. Il existe aujourd'hui des sites en production utilisant de manière plus ou moins étendues les Web Services, mais il faut encore à l'heure actuelle peser le pour et le contre au cas par cas, les travaux de standardisation sur certains aspects étant encore en cours.

Le standard SOAP 1.2 vient d'être recommandé (juin 2003) par le W3C. Ainsi il est proposé de préconiser dans le référentiel courant (v2.1) du cadre commun d'interopérabilité deux des principaux composants des Services WEB : SOAP et WSDL. Le composant UDDI, restant quant à lui encore en observation.

1.5.1.1 Les Services Web et la sécurité

Émergeants au rythme soutenu des nouvelles propositions de ses principaux contributeurs, les Web Services apportent leur lot de préoccupations, notamment en matière de sécurité.

Tout d'abord, leur encapsulation fréquente au sein du protocole HTTP, bien que judicieuse pour des besoins d'échange, rendent inefficaces les solutions de protections habituelles. De nouveaux coupe-feu analysant les messages SOAP voient progressivement le jour afin d'y remédier.

De plus, l'absence volontaire de fonctions de sécurité au niveau de SOAP freinait jusqu'à présent leur déploiement hors du contexte fermé de l'entreprise malgré l'émergence d'initiatives telles que la

standardisation des fonctions de signature (XML-Signature) et chiffrement (XML- Encryption) de documents XML.

Sur ce point WS Security fournit une approche cohérente afin de permettre l'authentification et l'intégrité des messages ainsi que leur confidentialité afin de fournir une sécurité de bout en bout. Pour ce faire, WS Security s'appuie sur les spécifications XML encryption, XML Signature et SAML (cf. chapitre 1.3 « Intégration des données » page 31). Ces spécifications restent néanmoins toujours adaptées pour sécuriser un service accédé par un demandeur.

Le problème de l'utilisation des seules spécifications de base (XML Encryption, XML Signature, SAML) survient lorsqu'une combinaison d'informations de signature, de chiffrement et d'authentification est utilisée dans un message SOAP ; dans ce cas, il n'y a pas d'informations sur le séquençement lié à leur traitement. En l'absence d'informations sur l'ordre dans lequel le message a été signé, chiffré ou authentifié, il y a une possibilité pour que le déchiffrement du message ou l'authentification de l'émetteur n'aboutisse pas. WS Security introduit des en-têtes de sécurité qui peuvent (et doivent) être utilisés pour contenir toutes les informations précédentes et préciser l'ordre dans lequel les informations de sécurité doivent être traitées.

Jusqu'à WS Security aucun mécanisme standardisé pour le transport des informations d'authentification dans un message Web Service n'existait. Certains Web services ont utilisé SSL avec authentification du client, ou les mécanismes de type HTTP Basic/Digest ou NTLM pour authentifier le message au niveau de la couche transport. D'autres ont inséré des paramètres SOAP arbitraires afin de transporter des données de type identifiant/mot de passe, avec un contrat implicite entre le client et le serveur afin d'assurer la compréhension de ces paramètres. De son côté WS Security introduit différents types de jetons de sécurité standardisés tels que les jetons UserNamePassword, les jetons binaires (Certificats X.509, tickets Kerberos), ou les jetons XML (SAML), pour passer ces informations.

En ce qui concerne la signature des messages XML, WS Security recommande des méthodes spécifiques pour leur réalisation et leur vérification afin de supporter les différentes options proposées par XML Signature. De plus, lorsque plusieurs parties d'un message SOAP sont signées avec la même clé, la clé publique utilisée pour vérifier ces messages ne doit être définie qu'une seule fois dans le message en faisant référence au jeton binaire pour les certificats X.509. Cela permet de réduire la taille du payload (ou champ utile du message).

De même, les parties des messages SOAP qui doivent être déchiffrées par une entité particulière sont spécifiées dans les en-têtes de sécurité. Les clés de chiffrement partagées doivent également être définies une seule fois dans le message plutôt qu'avec chaque donnée chiffrée, ce afin de réduire la taille des données utiles.

Certaines informations de sécurité SOAP, telles les tickets de service Kerberos ou les déclarations SAML) peuvent être valides uniquement pour des durées spécifiques. WS Security fournit des en-têtes standardisés qui peuvent être utilisés afin de déterminer la durée de validité du message.

Enfin, WS Security fournit des codes d'erreur standardisés qui peuvent être utilisés pour propager des informations lors des traitements des en-têtes de sécurité, par exemple un échec d'authentification ou le manque de données de sécurité.

Ainsi, WS Security dynamise et améliore plusieurs des spécifications existantes afin que les informations de sécurité puissent être créées et traitées de manière plus standardisée, afin de permettre l'interopérabilité entre les Web Services.

1.5.2 La technologie J2EE (le standard 1.3)

Java 2 Enterprise Edition est le modèle de composants promu par Sun et ses partenaires pour les applications d'entreprise. Il existe d'autres modèles de composants Java plus simples, pour les applications embarquées par exemple (J2ME) ou J2SE pour le poste client, mais elles n'entrent pas dans le champ de ce document.

J2EE est du point de vue marketing le nom phare autour duquel se structure l'affrontement économique avec Microsoft .NET.

J2EE au sens strict est une spécification, pas une implémentation. Cette spécification est contrôlée par Sun Microsystems. Il ne s'agit donc nullement d'un standard au sens formel. L'évolution de J2EE est régie par une charte, le Java Community Process (JCP), qui a été négociée entre Sun et ses partenaires.

J2EE n'est pas un standard en soi, mais un ensemble de standards ayant leur cycle de vie propre. A un instant donné, un ensemble cohérent est baptisé « J2EE version x.y » :

La dernière version publiée est J2EE 1.3 (Automne 2001) qui contient l'ensemble d'APIs suivants (par ordre alphabétique) :

- EJB (Enterprise JavaBeans) 2.0
- JAAS (Java Authentication and Authorization Service) 1.0
- JavaMail 1.1
- Java RMI (Remote Method Invocation) 1.0
- JAXP (the Java API for XML Processing) 1.1
- JDBC (Java Database Connectivity) 2.0
- JMS (Java Message Service) 1.0.2
- JNDI (Java Naming and Directory Interface) 1.2
- JSP (JavaServer Pages) 1.2
- JTA (Java Transaction API) 1.0.1
- J2EE Connector Architecture 1.0
- RMI/IIOP (Internet Inter-ORB Protocol) 1.0
- Servlets 2.3

Ces éléments sont considérés comme suffisamment stables et fortement répandus. Ils font l'unanimité sur le marché et sont largement utilisés par toutes les populations de création des applications informatiques. La prochaine version, J2EE 1.4, est depuis Août 2002 à l'état de « final draft ». Les évolutions sont centrées autour des points suivants :

- Support des Services Web : JAX-RPC, JAXR, SAAJ
- Support de XML : JAXP
- Management : JMX
- EJB 2.1
- JCA 1.5

1.5.3 La technologie .NET

.NET est une marque de Microsoft, un qualificatif pour les produits Windows et Visual Studio, Visual Basic, ASP, ADO ..., mais ni une spécification, ni un standard formel. C'est néanmoins un facteur majeur sur le marché pour l'architecture applicative. C'est un nouveau modèle de programmation, sensiblement différent du modèle traditionnel de Microsoft, avec des stratégies et des outils de migration.

L'architecture .NET est composée de plusieurs éléments :

- La CLR (Common Language Runtime), qui est une machine d'exécution virtuelle inspirée de la JVM de J2EE,
- La FCL (Framework Class Library), une collection de classes, structures et énumérations,

- Le .NET Framework SDK, qui regroupe un ensemble de compilateurs et d'outils permettant de développer les applications qui seront exécutées par la CLR.

Dans ce document, .NET désigne donc les applications écrites nativement avec VisualStudio.NET (l'environnement de développement) en VisualC#.NET ou en VisualBasic.NET. C# est un langage objet très similaire à Java. VB.NET est une évolution très significative de Visual Basic vers l'objet.

Ces applications sont ensuite exécutées sur Windows 2000 (avec un certains nombre de compléments) et prochainement sur Windows .NET, la nouvelle version serveur de Windows.

Il n'existe bien sûr qu'un seul .NET, celui de Microsoft, actuellement disponible sur Windows 2000 et en natif sur Windows .NET. La date de GA (General Availability) de Windows .NET est prévue en début 2003. Ceci montre la relative jeunesse de la plate-forme .NET, bien qu'il soit possible de faire du .NET soit avec Windows 2000 soit avec les pre-releases de Windows .NET.

Il existe un projet d'émulation de .NET en libre, MONO. L'opinion des auteurs de ce projet est assez partagée. Certains experts disent qu'il est quasiment impossible de faire le « reverse engineering » d'une architecture aussi évoluée que .NET sans la complicité de Microsoft et d'autres pensent que ce projet est prometteur et qu'il commence à donner des résultats. Il ne faut pas comparer cela à SAMBA par exemple qui a réussi sur le segment très bien défini d'un système de fichiers distribué.

1.5.4 La technologie ZOPE du monde des logiciels libres

Au même titre que J2EE ou .NET, Zope est une architecture à part entière.

Il propose un modèle « n-tiers », c'est à dire une claire séparation entre les données, la logique et la présentation ainsi qu'une infrastructure incluant un modèle de sécurité (contrairement à des systèmes où la sécurité est réalisée par programmation).

Il offre un accès natif et interchangeable aux bases de données relationnelles.

Son architecture permet la prise en charge de manière transparente de fonctions essentielles telles que la persistance des objets, l'intégrité des données, les contrôles d'accès, la gestion des transactions, la gestion des sessions, etc.

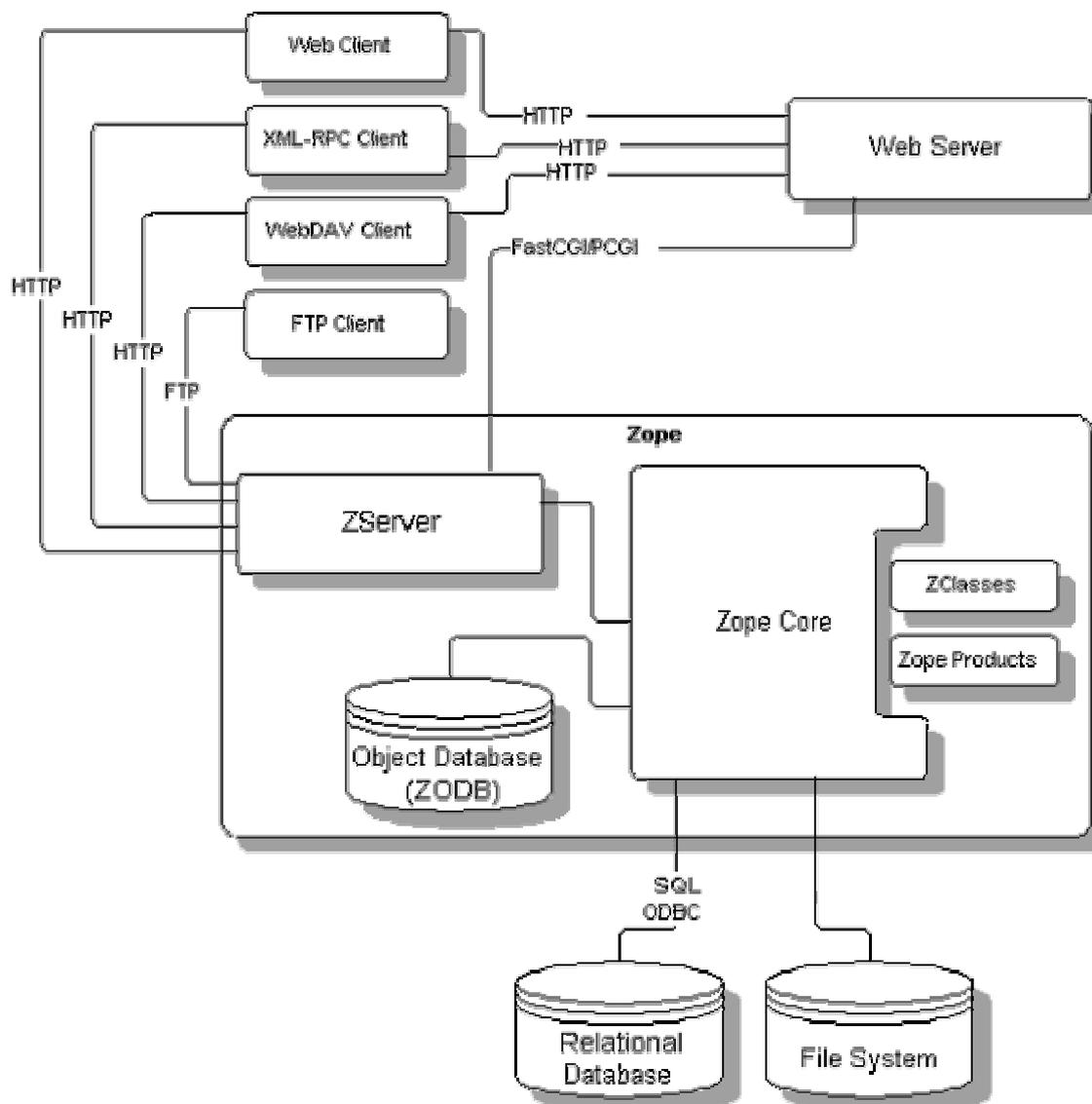
Son modèle orienté objet permet la création de composants métiers réutilisables (équivalent fonctionnel des beans) dont l'intégration à des architectures Zope déjà en place permet l'extension des modèles existants de manière native, cohérente, sécurisée et sans programmation.

La réplication d'objets et leur montée en charge de manière transparente et immédiate sans modification (composant de cluster Zope Enterprise Object – ZEO) sont également possibles.

Certains de ses éléments peuvent également être utilisés hors de l'architecture Zope (ZPT, base de donnée objet ZODB, etc ...).

Cette architecture n'étant pas traitée dans l'étude analytique des architectures applicatives (annexe 6) a fait l'objet dans le cadre du présent rapport d'une étude complémentaire (voir paragraphes suivants)

1.5.4.1 Le modèle d'architecture de ZOPE



1.5.4.2 Les composants majeurs de ZOPE

1.5.4.2.1 ZServer

ZServer offre une connectivité Internet souple supportant de nombreux protocoles réseau dont HTTP, FTP, XML-RPC, FastCGI, et PCGI. ZServer peut fonctionner en tandem avec des serveurs Web existants.

1.5.4.2.2 Zope Core

Zope contient un gestionnaire ORB Web, un moteur de recherche, une couche de sécurité et permet l'affiliation et le partage d'informations dynamiques.

1.5.4.2.3 Base de données Objet (ZODB)

La base de données objet, ZODB, qui supporte les transactions, l'annulation, les versions individuelles, peut aller jusqu'à plusieurs gigaoctets de données. Il existe également une option pour les entreprises qui permet extensibilité et basculement.

1.5.4.2.4 Intégration SGBDR

Zope offre une connexion conviviale et puissante aux grandes bases de données dont : Oracle, Sybase, MySQL, PostgreSQL, ainsi que des pilotes ODBC.

1.5.4.2.5 Zope Products

Zope Products offre de nouveaux types d'objets et des outils personnalisables écrits en Python.

1.5.4.2.6 ZClasses

ZClasses propose de nouveaux types d'objets créés via le Web. ZClasses ne nécessite aucune programmation. Sa distribution et son installation sont aisées.

1.5.4.3 L'architecture Zope et le respect des normes et standards ouverts

L'architecture Zope utilise de manière native uniquement des standards ouverts et est compatible (voire utilise également de manière native) la quasi totalité des standards retenus par le Cadre Commun d'Interopérabilité.

Les objets de la plate-forme Zope sont accessibles via les protocoles de communication : HTTP 1.0, HTTP 1.1, FTP, XML-RPC, SOAP, WebDav, FastCGI et même POP.

La base objet de Zope utilise de manière native le format XML (import, export).

Les formats Bureautique HTML, RTF, PDF, TIFF, PNG, GIF, JPEG, MP3, WAV sont supportés en natif.

Les formats XML et CSV sont utilisés en natif.

L'ensemble des protocoles d'interconnectivité IP, FTP, DNS, TCP, Wi-Fi LDAP, NNTP sont utilisés en natif.

XML-RPC et une première implémentation de SOAP sont disponibles en natif.

Les formats SGML, XML, XML/RDF/RSS, DOM, CSS, HTML4, LaTeX, PDF sont également utilisables.

L'architecture Zope est multi plate-forme et fonctionne de manière native et identique sous les systèmes d'exploitation :

- Windows : 95, 98, NT, 2000, XP
- Linux : Red Hat, Mandrake, Debian, SuSE, Caldera, OpenLinux, Gentoo, etc ...

- BSD : OpenBSD, NetBSD, FreeBSD
- Solaris
- Mac

L'architecture Zope est :

- multi-serveur et fonctionne de manière native et identique avec les serveurs Web Apache, Squid, Microsoft IIS, Iplanet, Netscape, Roxen, etc ...
- multi back-end, la base de donnée objet de Zope (ZOBD) pouvant indifféremment utiliser un back-end Zope, Oracle, SleepyCat, FileSystem, etc.
- multi-SGBDR, l'architecture modulaire et objet de Zope permettant de remplacer un SGBDR par un autre sans modification de la logique de traitement, des requêtes standards.
- multi-référentiel, les référentiels de sécurité, d'identification, d'authentification pouvant fonctionner indifféremment à partir d'une base Zope, d'une base LDAP, d'une base SQL, des services d'authentification de windows NT, etc. Le changement de référentiel peut intervenir sans modification des applications.
- multi-langage, et scriptable via de nombreux langages : DHTML, Python, Perl, ... ainsi que via COM, CORBA, .NET soit en natif soit via une encapsulation (wrapper).

L'architecture Zope peut répondre à un large spectre de la typologie applicative :

- Web interactif : y compris pour les applicatifs « mission critical » comme celle de tous les postes de commandement de l'OTAN pour lesquels Zope sert d'infrastructure d'intégration.
- Publication : comme par exemple le site à très haut trafic www.cbsnewyork.com, ou le site Internet du Ministère de l'Intérieur.
- Décisionnel : comme par exemple l'analyse financière stratégique par Quantax.
- Collaboratif : comme le SIT du Bas-Rhin qui utilise Zope comme base de travail collaboratif, et comme base de mise en place de guichets uniques.

1.5.4.4 L'architecture ZOPE vis à vis des normes, standards et architectures du moment

L'architecture Zope ne repose sur aucun standard ni spécification propriétaire.

Elle est adaptée à la capacité de de générer du HTML, de produire et consommer du XML, de produire et consommer des services Web.

L'architecture Zope est adaptée à la construction d'une architecture de composants génériques et de composants métiers réutilisables. Elle a la capacité à intégrer de nouveaux standards et à interopérer avec le monde J2EE et le monde .NET.

1.5.5 Standards applicables

Composant	Standard	RFC	Date / Version	Etat du standard	Commentaires
Protocole d'accès à distance : SOAP	SOAP 1.1	http://www.w3.org/TR/SOAP	mai-00	Note	
	SOAP 1.2	http://www.w3.org/TR/soap12-part1/ http://www.w3.org/TR/soap12-part2/	Juin 2003	Recommandé	
Description des services	WSDL	http://www.w3.org/TR/wsdl http://www.w3.org/TR/wsdl12	v1.1 : mars 2001 v1.2 : juin 2003	v1.1 : Note v1.2 : Draft	

1.5.6 Candidats au référentiel Vx

Composant	Standard	RFC	Date / Version	Etat du standard	Commentaires
Sécurité Services Web	WS-Security	N/A	déc-02	Document de travail	Spécifications WS Security http://www.oasis-open.org/committees/wss/documents/WSS-Core-08-1212-merged.pdf
		N/A	sept-02	Document de travail	Support de Kerberos http://www.oasis-open.org/committees/wss/documents/WSS-Kerberos.pdf
		N/A	déc-02	Document de travail	Support de SAML http://www.oasis-open.org/committees/wss/documents/WSS-SAML-05.pdf
		N/A	sept-02	Document de travail	Support des certificats X.509 http://www.oasis-open.org/committees/wss/documents/WSS-X509.pdf
		N/A	sept-02	Document de travail	Support de XrML http://www.oasis-open.org/committees/wss/documents/WSS-XrML-01.pdf
		N/A	nov-02	Document de travail	Support de XCBF http://www.oasis-open.org/committees/wss/documents/WSS-XCBF.pdf
Description de répertoire des	UDDI	N/A	v2 : juillet 2002 v3 :		http://www.uddi.org/ A suivre pour prise en compte ultérieure.



Cadre commun d'interopérabilité
version 2.1
Mise à jour des standards et des référentiels

services			juillet 2002		
-----------------	--	--	-----------------	--	--

2 Récapitulatif des mises à jour proposées pour la version 2 du CCI

2.1 INTERCONNECTIVITE

2.1.1 Les standards proposés pour suppression

2.1.1.1 Suppression de standards du référentiel

Composant	Version CCI	Standard	RFC	Date / Version	Etat du standard	Commentaires
Messagerie	V1	SMTP	RFC 821	août-82	Standard	rendu obsolète par le RFC 2821
	V1	SMTP ARPA	RFC 822	août-82	Standard	rendu obsolète par le RFC 2822
	V1	ESMTP	RFC 1869	novembre-95	Standard	rendu obsolète par le RFC 2821
Sécurité des outils de messagerie électronique	V1	S/MIME	RFC 2630	juin-99	Proposé	rendu obsolète par les RFC 3369 et 3370

2.1.1.2 Suppression de candidats aux versions ultérieures

Composant	Version CCI	Standard	RFC	Date / Version	Etat du standard	Commentaires
Infrastructure de Gestion des Clés	Vx	X.509	RFC 2459	janvier-99	Proposé	Rendue obsolète pas la RFC 3280
			RFC 1428	février-93	Informatif	N'a aucune vocation de standard
Newsgroups	Vx	NNTP	RFC 2980	octobre-00	Informatif	N'a aucune vocation de standard
Infrastructure de gestion de clés	Vx	PKI	PKCS#7			Rien à faire dans la PKI. La signature est traitée au niveau des applications qui la mettent en
	Vx		Signature électronique			

2.1.2 Les standards proposés en complément

2.1.2.1 Compléments au référentiel courant

Composant	Version CCI	Standard	RFC	Date / Version	Etat du standard	Commentaires
Réseaux sans fil	v2	Wi-Fi	IEEE 802.11b	févr-00	Standard	Version actuellement déployée
Infrastructure de gestion de clés	v2	PKI	RFC 2510 & 2511 (X509)	mars-99	Proposé	Protocole et format de message pour une demande de création de certificat à une AC
	v2		RFC 2559	avril-99	Proposé	Utilisation de LDAPv2 dans une PKI
	v2		RFC 2560 (OCSP)	juin-99	Proposé	OCSP
	v2		RFC 2585	mai-99	Proposé	Utilisation de FTP et HTTP afin de récupérer un certificat ou une CRL
	v2		RFC 2587	juin-99	Proposé	Schéma LDAPv2 pour une PKI
Protocole de transfert de fichiers	v2		RFC 2985	novembre-00	Information	PKCS #9 v2.0 (RSA)
	v2	FTP	RFC 2773	février-00	Experimental	
Outils de messagerie électronique	v2	MIME	RFC 3335	septembre-02	Proposé	Echange de messages EDI avec MIME
	v2		RFC 1870	septembre-97	Standard	Mise à jour V2 : appel à commentaires
	v2	ESMTP	RFC 2920	septembre-00	Standard	
Sécurité des outils de messagerie électronique	v2	S/MIME	RFC 3369	août-02	Proposé	Définit la syntaxe pour signer, condenser, authentifier ou chiffrer le contenu d'un message
	v2		RFC 3370	août-02	Proposé	Définit les conventions d'utilisation des algorithmes de cryptographie
Annuaire	v2	LDAP V3	RFC 2252 - 2256	décembre-97	Proposé	Mise à jour V2 : nécessaire à l'interopérabilité
	v2		RFC 2649	août-99	Expérimental	Control et schéma LDAP pour les opérations de signature
	v2		RFC 2820	mai-00	Information	Contrôle d'accès pour LDAP
	v2	Extensions LDAP	RFC 2798	avril-00	information	Mise à jour V2 : cohérence du référentiel MAIA
	v2		RFC 2247	janvier-98	Proposé	
	v2	LDIF	RFC 2849	juin-00	Proposé	
	v2	attribut X.400	RFC 2294	mars-98	Proposé	
	v2	rfc822mailbox	RFC 1274	novembre-91	Proposé	
	v2	LabelledURI	RFC2079	janvier-97	Proposé	
	v2	repérageURI	RFC 2396	août-98	Proposé	
	v2		RFC 2829	mai-00	Proposé	Méthodes d'authentification pour LDAP
	v2		RFC 2830	mai-00	Proposé	Extension LDAPv3 pour TLS
	v2		RFC 3377	septembre-02	Proposé	Spécifications Techniques LDAPv3



Premier ministre

ATICA

Cadre commun d'interopérabilité

version 2.1

Mise à jour des standards et des référentiels

2.1.2.2 Complément de candidats aux versions ultérieures

Composant	Version CC*	Standard ^d	RFC	Date / Versio ⁿ	Etat du standard	Commentaires	Référentiels
LAN/WAN interconnexion	Vx	IPv6	RFC 2373	juillet-98	Proposé	Attente de la prise en compte effective par les marchés. Infos IPv6 : http://www.ipv6.org/v6-apps.html	
	Vx		RFC 2374	juillet-98	Proposé		
	Vx		RFC 2460	décembre-98	Draft		
	Vx		RFC 2461	décembre-98	Draft		
	Vx		RFC 2462	décembre-98	Draft		
	Vx		RFC 2463	décembre-98	Draft		
	Vx		RFC 2675		Proposé	Mise à jour V2 : paquets gros volumes	
	Vx	Transition IPv4-IPv6	RFC 2893	août-00	Proposé		Référentiel Transition IPv6 à prévoir ultérieurement
	Vx		RFC 2766	février-00	Proposé		
	Vx	FTP	RFC 2428		Proposé	Mise à jour V2 : extensions IPv6	
	Vx	DNS	RFC 1886		Proposé		
	Vx	DNSSec	RFC 3226		Proposé	Support des enregistrements DNSSec et des adresses IPv6	
	Vx		RFC 3445		Proposé	Limitation du champ d'action du Ressource Record KEY	
	Vx	TCP	RFC 2018		Proposé	Mise à jour V2 : options proposées	
	Vx		RFC 2581		Proposé		
	Vx		RFC 2873		Proposé		
	Vx		RFC 2883		Proposé		
	Vx		RFC 3042		Proposé		
Vx		RFC 3168		Proposé			
Vx		RFC 3390		Proposé			
Vx	Wi-Fi	IEEE 802.11g		sept-00	New Std Project	Version émergente	
Vx		IEEE 802.11i		May 2001	En cours	Intègre la sécurité WPA.	
Infrastructure de gestion de clés	Vx	PKI	RFC 3279	janvier-99	Proposé	Algorithmes et identifiants pour le profile des certificats et des CRL	A prévoir dans un référentiel d'architecture de confiance et description des procédures à respecter.
	Vx		RFC 3280	mars-99	Proposé	Profile des certificats et des CRL	
	Vx		RFC 3281	avril-99	Proposé	Profile de certificat d'attribut pour l'autorisation	
Qualité de Service	Vx	DiffServ	RFC 2474	décembre-98	Proposé		
	Vx		RFC 2597	juin-99	Proposé		
	Vx		RFC 2598	juin-99	Proposé		
	Vx	RSVP	RFC 2205	septembre-97	Proposé		
	Vx		RFC 2680	septembre-99	Proposé		
	Vx		RFC 2679	septembre-99	Proposé		
Annuaire	Vx	x500	RFC 2459, RFC 2510, RFC 2527 et ETSI 101862, ETSI 10173			Normes abandonnées au profit de LDAP (à confirmer pour protocole DSP)	
	Vx	X 501					
	Vx	X 509				Voir Sécurité et PKI	
	Vx	Extensions LDAP	RFC 2927	septembre-00	information		
	Vx		RFC 2377	septembre-98	information	cohérence avec le référentiel MAIA	
	Vx		RFC 2307	mars-98	expérimental		
Vx	RFC 1617	mai-94	information				
Newsgroup	Vx	NNTP	RFC 977	février-86	Proposé		

2.2 DONNEES

2.2.1 Les standards proposés pour suppression

2.2.1.1 Suppression de standards du référentiel

Aucun candidat aux versions ultérieures n'est supprimé

2.2.1.2 Suppression de candidats aux versions ultérieures

Composant	Version CCI	Standard	RFC	Commentaires
Sécurité des données	Vx	Signature XML	http://www.w3.org/Signature/	A suivre pour prise en compte ultérieure (lorsque le standard sera industriellement reconnu)

2.2.2 Les standards proposés en complément

2.2.2.1 Compléments au référentiel courant

Composant	Version CCI	Standard	RFC	Date / Version	Etat du standard	Commentaires
Sécurité XML	v2	XML Signature XMLSIG	N/A	février-02	Recommandation W3C	XML Signature Syntax and Processing - http://www.w3.org/TR/2002/REC-xmlsig-core-20020212/
			RFC 2807	juillet-00	Information	XML Signature Requirements
			RFC 3275	mars-02	Proposé	XML Signature Syntax and Processing
	v2	XML Encryption XMLENC	N/A	mars-02	Draft W3C	XML Encryption Requirements - http://www.w3.org/TR/xml-encryption-req
			N/A	décembre-02	Draft W3C	XML Encryption Syntax and Processing - http://www.w3.org/TR/xml-encryption-req
			N/A	décembre-02	Draft W3C	Decryption Transform for XML Signature - http://www.w3.org/TR/xmlenc-decrypt

2.2.2.2 Complément de candidats aux versions ultérieures

2.3 FORMATS ET SUPPORTS

2.3.1 Les standards proposés pour suppression

2.3.1.1 Suppression de standards du référentiel

Composant	Version CCI	Standard	Etat du standard	Commentaires
Echange d'information graphique/images fixes	V0	UIT T4	Recommandé, - pérenne, - ouvert, - très utilisé	Ce format est un dérivé du format TIFF. Il est le plus répandu grâce à son exploitation par les télécopieurs.
Echange d'images animées / information audiovisuelle	V0	MPEG 3	Recommandé, - pérenne, - ouvert, - très utilisé	MPEG 3 Cette norme est une évolution de MPEG 2 et utilise uniquement la partie relative au son. Le son est stéréophonique.
Base de données	V0	Texte plat	Recommandé, - pérenne, - ouvert, - très utilisé	Le contenu des bases de données est à conserver sous la forme d'un texte à plat doté de séparateurs (virgule de séparation).

2.3.1.2 Suppression de candidats aux versions ultérieures

Aucun candidat aux versions ultérieures n'est supprimé.

2.3.2 Les standards dont l'Etat a subi une évolution

Des changements de recommandation sont effectués pour certains standards : passage de « possible » à « recommandé », ou l'inverse.

Composant	Version CCI	Standard	RFC	Date / Version	Etat du standard	Commentaires
Jeux de caractères et alphabets	V0	UNICODE	http://www.unicode.org/standard	v3.2 mars 2002	Recommandé, - pérenne, - ouvert, - utilisé	Unicode est un sur-ensemble de la norme ISO 10646-1 - Universal Multiple-Octet Coded Character Set (UCS), dans sa version restreinte au codage sur deux caractères. Les 256 premières valeurs de la norme ISO 10646-1 correspondent à la norme ISO 8859-1 latin 1.
	V0	TXT			Possible, - pérenne, - ouvert, - très utilisé	Les fichiers textes sont pérennes car très simples, mais ils induisent une perte d'information sensible. D'autre part le codage des fins de lignes n'est pas standardisé. Il est conseillé de les migrer vers XML.
Formats de documents	V0	XML	http://www.w3.org/TR/2000/REC-xml-20001006	1.0 06/10/2000	Recommandé, - pérenne, - ouvert, - utilisé	XML (Extensible Mark-Up Language) est basé sur SGML. Il a été conçu et promu par l'association W3C (World Wide Web Consortium) qui est le référent dans le domaine Internet. Par exemple, les différents composants de la suite bureautique OpenOffice.org stockent leurs données au format XML.
	V0	RTF	http://msdn.microsoft.com/library/en-us/dnrtf/spec/html/rtfspec.asp	v1.6 mai 1999	Possible, - pérenne, - propriétaire, - très utilisé	Le format RTF (ou Rich Text Format) est un format propriétaire de Microsoft, destiné à l'échange de documents.
	V0	PDF	http://www.adobe.fr/products/acrobat/adbepdf.html	v5.0	Possible, - pérenne, - propriétaire, - très utilisé	Le format PDF, ou Portable Document Format, est un format propriétaire de la société Adobe, lié au logiciel Acrobat. Son usage est très répandu. Adobe diffuse actuellement gratuitement le logiciel de lecture Acrobat Reader, sous réserve de l'acceptation de la licence. (http://www.adobe.fr/products/acrobat/acrcrula.html)
Echange d'information graphique/ images fixes	V0	TIFF	http://www.itu.int	v6.0	Possible, - pérenne, - ouvert, - très utilisé	TIFF (Tag Image File Format) Groupe IV est une norme de l'Union Internationale des Télécommunications (UIT). Ce format est très répandu grâce à son exploitation par les télécopieurs et par les scanners. Il utilise des types de compression permettant de garantir la qualité et l'absence de perte.
	V0	GIF	http://www.compuserve.com http://www.unisys.com		Possible, - peu pérenne, - propriétaire, - faiblement utilisé	GIF (Graphic Interchange Format) est un format très répandu. Ce format étant propriétaire, il y a lieu de veiller à migrer dès que possible les fichiers GIF en fichiers PNG.
	V0	JPEG	http://www.jpeg.org		Recommandé, - pérenne, - ouvert, - très utilisé	JPEG (Joint Photographic Experts Group). Cette norme, définie par l'ISO, est très utilisée pour la photographie numérique. Elle permet un haut niveau de compression (de l'ordre de 1/40). La contrepartie est une perte d'information.
Flux audiovisuels	V0	MP3	http://www.mpeg.org		Recommandé, - pérenne, - ouvert, - très utilisé	MP3, abrégé de MPEG-1 Layer III Audio, est une norme de compression du son stéréophonique. MP3 est très répandu. Cette norme intègre cependant des algorithmes brevetés.
	V0	WAV			Possible, - peu pérenne, - propriétaire, - faiblement utilisé	WAV (RIFF WAVE). À l'origine, format de fichier sonore de Microsoft Windows, il est maintenant élargi à d'autres plates-formes. Le son est stéréophonique.
	V0	MPEG-2	http://www.mpeg.org		Recommandé, - pérenne, - ouvert, - très utilisé	MPEG-2 (Moving Picture Expert Group). Cette norme de compression pour les images animées fonctionne sur toutes les plates-formes. Cette norme intègre cependant des algorithmes brevetés.
Plans	V0	STEP	http://www.iso.ch	ISO 10303	Recommandé, - pérenne, - ouvert, - utilisé	STEP (Standard for the Exchange of Product Data). Normes pour l'échange d'informations sur les produits industriels. Ces normes sont répandues.
	V0	DXF			Possible, - pérenne, - propriétaire, - très utilisé	DXF, format propriétaire utilisé par le logiciel Autocad qui est très répandu.

2.3.3 Les standards proposés en complément

2.3.3.1 Compléments au référentiel courant

Composant	Version CCI	Standard	RFC	Date / Version	Etat du standard	Commentaires
Flux audiovisuels	v2	MPEG-4	http://www.mpeg.org	ISO/IEC 14496 V2 2000	Recommandé, - pérenne, - ouvert, - utilisé	MPEG-4 est une norme de compression pour les images animées, définie par le Moving Picture Expert Group de l'ISO. Le dernier niveau du standard est aussi nommé H264 par l'UIT. MPEG-4 permet de gérer des flux pour l'accès à travers internet et la visioconférence. DivX, parfois assimilé à tort à MPEG-4, est en fait basé sur MPEG-4 Visual pour l'image et MP3 pour le son.
	v2	DV	http://www.dvformat.com		Possible, - pérenne, - ouvert, - très utilisé	DV (Digital Video cassette) est un format d'acquisition vidéo défini par un consortium de sociétés.
Echange de bases de données	v2	XML	http://www.w3.org/XML		Recommandé, - pérenne, - ouvert, - utilisé	Il est recommandé d'utiliser XML pour les échanges de bases de données.
Echange de bases de données	v2	CSV			Possible, - pérenne, - ouvert, - très utilisé	CSV (Comma Separated Values) Le contenu des bases de données peut être mis sous la forme d'un texte "à plat" doté de séparateurs (virgule de séparation).

2.3.3.2 Complément de candidats aux versions ultérieures

Composant	Version CCI	Standard	RFC	Date / Version	Etat du standard	Commentaires
Formats de documents	vx	XHTML	http://www.w3.org/TR/xhtml1/		A prendre en compte dans une version ultérieure du CCI	XHTML est une recommandation du World Wide Web Consortium, définie le 26/01/2000 et mise à jour le 01/08/2002. Elle est basée sur XML et définit une syntaxe proche de HTML 4.0 mais plus contrainte.
	vx	OASIS Open Office XML Format	http://www.oasis-open.org/committees/office		A prendre en compte dans une version ultérieure du CCI	OASIS a constitué un groupe de travail pour normaliser un format d'échange de documents basé sur XML, en prenant comme base le format utilisé par OpenOffice.org.
	vx	Microsoft Office v11 XML Format	http://www.microsoft.com/office/development/preview/XML.asp		A prendre en compte dans une version ultérieure du CCI	Microsoft annonce pour la version 11 d'Office, une intégration forte de XML. Les composants d'Office pourront lire et produire au format XML. La disponibilité des spécifications d'interface d'Office 11 est un pré-requis pour la prise en compte dans une version ultérieure du CCI.
	vx	PDF/A	http://www.aiim.org/pdf_a		A prendre en compte dans une version ultérieure du CCI	NPES (The Association for Suppliers of Printing, Publishing and Converting Technologies) et AIIM International (Association for Information and Image Management, International) se sont associés pour définir un format d'archivage pérenne, nommé PDF/A et basé sur le format PDF d'Adobe.
	vx	XForms	http://www.w3.org/TR/xforms-Candidate-Recommendation-20/11/2002		A prendre en compte dans une version ultérieure du CCI	XForms est une recommandation candidate du World Wide Web Consortium, définie le 20/11/2002. Elle est basée sur XML et permet la réalisation de formulaires. XForms gère séparément la présentation et le contenu. XForms permet le typage des données à saisir. Cette norme n'est pas un nouveau type de document, mais est conçue pour être intégrée dans des langages comme XHTML ou SVG.
Images fixes	vx	SVG	http://www.w3.org/TR/svg-Recommendation-v1.0-04/09/2001		A prendre en compte dans une version ultérieure du CCI	SVG 1.0 (Scalable Vector Graphic) est une norme du World Wide Web Consortium, définie le 04/09/2001. Elle est basée sur XML et permet la description d'objets graphiques vectoriels en deux dimensions. Elle permet l'interactivité, le scripting et l'animation.
Flux de données audio	vx	Ogg Vorbis	http://www.vorbis.com http://vorbismusic.fr		A prendre en compte dans une version ultérieure du CCI	Ogg Vorbis est une technologie d'encodage, de lecture et de diffusion audio, distribuée en logiciel libre, sous licence GPL. Ogg Vorbis a pour objectif de remplacer le format MP3.
Echange de données audiovisuelles	vx	AAF	http://www.aafassociation.org		A prendre en compte dans une version ultérieure du CCI	AAF (Advanced Authoring Format/ Format d'édition avancé), a été développé par Avid et est proposé en format logiciel libre depuis 2000. AAF permet l'échange de données multimédias composites entre producteurs multimédia.
	vx	MPEG-4 part 10 / H.26L			Cette norme, en cours de définition, est proposée pour une version ultérieure du CCI.	ISO/MPEG et l'UIT élaborent actuellement MPEG-4 part 10 / H.26L, avec l'objectif d'une norme ne comprenant pas de versement de redevances (<i>royalty-free</i>).

2.4 LES ARCHITECTURES APPLICATIVES

2.4.1 Les standards proposés en complément

2.4.1.1 Compléments au référentiel courant

Composant	Version CCI	Standard	RFC	Date / Version	Etat du standard	Commentaires
Protocole d'accès à distance : SOAP	v2	SOAP 1.1	http://www.w3.org/TR/SOAP11/	mai-00	Note	
		SOAP 1.2	http://www.w3.org/TR/soap12-part1/ http://www.w3.org/TR/soap12-part2/	déc-02	Recommandé	
Description des services	v2	WSDL	http://www.w3.org/TR/wsdl12/	v1.1 : mars 2001 v1.2 : juin 2003	version 1.1 : Note version 1.2 : Draft	

2.4.1.2 Complément de candidats aux versions ultérieures

Composant	Version CCI	Standard	RFC	Date / Version	Etat du standard	Commentaires
Sécurité WS	Vx	WS-Security	N/A	déc-02	Document de travail	Spécifications WS Security http://www.oasis-open.org/committees/wss/documents/WSS-Core-08-1212-merged.pdf
	Vx		N/A	sept-02	Document de travail	Support de Kerberos http://www.oasis-open.org/committees/wss/documents/WSS-Kerberos.pdf
	Vx		N/A	déc-02	Document de travail	Support de SAML http://www.oasis-open.org/committees/wss/documents/WSS-SAML-05.pdf
	Vx		N/A	sept-02	Document de travail	Support des certificats X.509 http://www.oasis-open.org/committees/wss/documents/WSS-X509.pdf
	Vx		N/A	sept-02	Document de travail	Support de XrML http://www.oasis-open.org/committees/wss/documents/WSS-XrML-01.pdf
	Vx		N/A	nov-02	Document de travail	Support de XCBF http://www.oasis-open.org/committees/wss/documents/WSS-XCBF.pdf
Description de répertoire des services	Vx	UDDI	http://www.uddi.org/	v2 : juillet 2003 v3 : juillet 2003		A suivre pour prise en compte ultérieure

3 Conclusion

3.1 TABLEAUX DES STANDARDS INTEGRES DANS LA VERSION V2.1 DU CCI

Les tableaux suivants résument le cadre commun d'interopérabilité applicable (Version V2.1 de septembre 2003) issu des différentes discussions exposées dans les chapitres précédents.

3.1.1 Interconnectivité

Composant	Standard	RFC	Date / Version	Etat du standard	Commentaires
LAN/WAN interconnexion	IPv4	RFC 791	septembre-81	Standard	
Protocoles de Transport	TCP	RFC 793	septembre-81	Standard	Standard MIL-STD-1778
		RFC1323	mai-92	Proposé	Mise à jour V2 : performances haut débit
Protocole de transfert	HTTP v1.1	RFC 768	août-80	Standard	Imposer des contraintes de sécurité
		RFC 2616 RFC 2817	juin-99 mai-00	Draft Proposé	A prendre en compte. Compatibilité ascendante avec HTTP V1.0
	Wi-Fi	IEEE 802.11b	févr-00	Standard	Version actuellement déployée
Infrastructure de gestion de clés	PKI	RFC 2510 & 2511 (X509)	mars-99	Proposé	Protocole et format de message pour une demande de création de certificat à une AC
		RFC 2559	avril-99	Proposé	Utilisation de LDAPv2 dans une PKI
		RFC 2560 (OCSP)	juin-99	Proposé	OCSP
		RFC 2585	mai-99	Proposé	Utilisation de FTP et HTTP afin de récupérer un certificat ou une CRL
		RFC 2587	juin-99	Proposé	Schéma LDAPv2 pour une PKI
Protocole de transfert de fichiers	FTP	RFC 2985	novembre-00	Information	PKCS #9 v2.0 (RSA)
		RFC 959	octobre-85	Standard	très limité
		RFC 2228	octobre-97	Proposé	
		RFC 2640	juillet-99	Proposé	FTP est déconseillé en contexte Web
		RFC 2773 RFC 2389	février-00 août-00	Experimental Proposé	Mise à jour V2 : négociation des options
Serveur de noms de domaines	DNS	RFC 1034	novembre-87	Standard	
		RFC 1035	novembre-87	Standard	
		RFC 1101	avril-89	Non indiqué	Actualise les RFC 1034 et 1035
	DNSSEC	RFC 2535	mars-99	Proposé	Extension sécurité DNS
		RFC 2931 RFC 3007 RFC 3008	septembre-00 novembre-00 novembre-00	Proposé Proposé Proposé	Mise à jour de la signature des requêtes et réponses DNS Sécurisation des mises à jour DNS Autorité de signature DNSSEC
Outils de messagerie électronique	SMTP	RFC 2821	août-82	Standard	Mise à jour V2 : remplace le RFC 821
		RFC 2822 RFC 2156	août-82 janvier-98	Standard Proposé	Mise à jour V2 : remplace le RFC 822
	MIME	RFC 2045	novembre-96	Draft	Mise à jour par RFC 2184 et 2231
		RFC 2046	novembre-96	Draft	
		RFC 2047	novembre-96	Draft	Mise à jour par RFC 2184 et 2231
		RFC 2048 RFC 2049	novembre-96 novembre-96	Recommandé Draft	Interopérabilité selon configuration à répertoire
		RFC 3335	septembre-02	Proposé	Echange de messages EDI avec MIME
	ESMTP	RFC 1652	juillet-94	Draft	
		RFC 1891 RFC 1892 à 1894	janvier-96 janvier-96	Proposé Proposé	
		RFC 1870 RFC 2920	septembre-97 septembre-00	Standard Standard	Mise à jour V2 : appel à commentaires
Sécurité des outils de messagerie électronique	S/MIME	RFC 2632 à RFC 2634	juin-99	Proposé	
		RFC 3369	août-02	Proposé	Définit la syntaxe pour signer, condenser, authentifier ou chiffrer le contenu d'un message
Sécurité de transport	SSL v3/TLS	RFC 3370	août-02	Proposé	Définit les conventions d'utilisation des algorithmes de cryptographie
		RFC 2246 RFC 2401 à 2410 RFC 2411 et 2412	janvier-99 novembre-98 novembre-98	Proposé Proposé Informatif	Seul TLS est IETF
Annuaire	LDAP v3	RFC 2251	décembre-97	Proposé	
		RFC 2252 - 2256	décembre-97	Proposé	Mise à jour V2 : nécessaire à l'interopérabilité
		RFC 2649	août-99	Experimental	Control et schéma LDAP pour les opérations de signature
		RFC 2820	mai-00	Information	Contrôle d'accès pour LDAP
	Extensions LDAP	RFC 2798	avril-00	information	
		RFC 2247 RFC 2849	janvier-98 juin-00	Proposé Proposé	
	attribut X.400	RFC 2294	mars-98	Proposé	
		rfc822mailto	RFC 1274	novembre-91	Proposé
	LabelledURI	RFC 2079	janvier-97	Proposé	
		RFC 2396	août-98	Proposé	
	repérageURI	RFC 2829	mai-00	Proposé	Méthodes d'authentification pour LDAP
		RFC 2830	mai-00	Proposé	Extension LDAPv3 pour TLS
	RFC 3377	septembre-02	Proposé	Spécifications Techniques LDAPv3	
Accessibilité		Web Content Accessibility Guidelines 1.0			
		www.w3.org/TR/1999/AWAI-WEBCONTENT-19990505	mai-99		

3.1.2 Données

Composant	Standard	RFC	Date / Version	Etat du standard	Commentaires
Metadonnées Metalangage	XML (Extensible Markup Language)	http://www.w3.org/TR/REC-xml	V1.0	Recommandé	
Définition des métadonnées	Schémas XML	http://www.w3.org/TR/xmlschema-0/ http://www.w3.org/TR/xmlschema-1/ http://www.w3.org/TR/xmlschema-2/		Recommandé	
Outils de traitement et de présentation des données	XSL Transformations (XSLT)	V1.0	novembre-99	Recommandé	http://www.w3.org/TR/xslt/
Sécurité XML	XML Signature XMLSIG	N/A	février-02	Recommandation W3C	XML Signature Syntax and Processing - http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/
		RFC 2807	juillet-00	Information	XML Signature Requirements
		RFC 3275	mars-02	Proposé	XML Signature Syntax and Processing
	XML Encryption XMLENC	N/A	mars-02	Draft W3C	XML Encryption Requirements - http://www.w3.org/TR/xml-encryption-reg
		N/A	décembre-02	Draft W3C	XML Encryption Syntax and Processing - http://www.w3.org/TR/xml-encryption-reg
N/A	décembre-02	Draft W3C	Decryption Transform for XML Signature - http://www.w3.org/TR/xmlenc-decrypt		
Langage de description et de modélisation des données	UML	http://www.omg.org/uml/	sept. 2001 / v1.4	ouvert, très utilisé, standard OMG	UML (Unified Modeling Language) de l'OMG (Object management Group). Ce langage permet de modéliser les processus et les données

3.1.3 Formats et supports

Composant	Standard	RFC	Date / Version	Etat du standard	Commentaires
Jeux de caractères et alphabets	UNICODE	http://www.unicode.org/standard	v3.2 mars 2002	Recommandé, - pérenne, - ouvert, - utilisé	Unicode est un sur-ensemble de la norme ISO 10646-1 Universal Multiple-Octet Coded Character Set (UCS), dans sa version restreinte au codage sur deux caractères. Les 256 premières valeurs de la norme ISO 10646-1 correspondent à la norme ISO 8859-1.
Formats de documents	TXT			Possible, - pérenne, - ouvert, - très utilisé	Les fichiers textes sont pérennes car très simples, mais ils induisent une perte d'information sensible. D'autre part le codage des fins de lignes n'est pas standardisé. Il est conseillé de les migrer vers XML.
	XML	http://www.w3.org/TR/2000/REC-xml-20001006	1.0 06/10/2000	Recommandé, - pérenne, - ouvert, - utilisé	XML (extensible mark-up language) est basé sur SGML. Il a été conçu et promu par l'association W3C (World Wide Web Consortium) qui est le référent dans le domaine Internet. Par exemple, les différents composants de la suite bureautique OpenOffice.org stockent leurs données en XML.
	SGML	ISO 8879 : 1986	juin-05	Possible, - pérenne, - ouvert, - faiblement utilisé	SGML (Structured General Mark-Up Language) est un langage de description de documents. L'utilisation de XML, de préférence à SGML, est recommandée.
	HTML	http://www.w3.org/TR/html4	4.0.1 24/02/1999	Possible, - pérenne, - ouvert, - très utilisé	HTML (Hyper Text Mark-up Language) est à la base des applications Internet. Il peut être utilisé en tant que format d'échange, bien que le format recommandé soit XML. Il est recommandé de faire figurer le numéro de version ainsi que les feuilles de style utilisées.
	RTF	http://msdn.microsoft.com/library/en-us/dnrtf/spec/html/rtf/spec.asp	v1.6 mai 1999	Possible, - pérenne, - propriétaire, - très utilisé	Le format RTF (ou Rich Text Format) est un format propriétaire de Microsoft, destiné à l'échange de documents.
	PDF	http://www.adobe.fr/products/acrobat/adbepdf.html	v5.0	Possible, - pérenne, - propriétaire, - très utilisé	Le format PDF, ou Portable Document Format, est un format propriétaire de la société Adobe, lié au logiciel Acrobat. Son usage est très répandu. Adobe diffuse actuellement gratuitement le logiciel de lecture Acrobat Reader, sous réserve de l'acceptation de la licence.
Echange d'information graphique/ images fixes	TIFF	http://www.itu.int	v6.0	Possible, - pérenne, - ouvert, - très utilisé	TIFF (Tag Image File Format) Groupe IV est une norme de l'Union Internationale des Télécommunications (UIT). Ce format est très répandu grâce à son exploitation par les télécopieurs et par les scanners. Il utilise des types de compression permettant de garantir la qualité et l'absence de perte.
	PNG	http://www.libpng.org/pub/png/	v1.1 31/12/1998	Recommandé, - pérenne, - ouvert, - faiblement utilisé	PNG (Portable Network Graphics). Il vise à remplacer le format propriétaire GIF pour la compression sans pertes. Ce format est promu par l'association W3C.
	GIF	http://www.compuserve.com http://www.unisys.com		Possible, - peu pérenne, - propriétaire, - faiblement utilisé	GIF (Graphic Interchange Format) est un format très répandu. Ce format étant propriétaire, il y a lieu de veiller à migrer dès que possible les fichiers GIF en fichiers PNG.
	JPEG	http://www.jpeg.org		Recommandé, - pérenne, - ouvert, - très utilisé	JPEG (Joint Photographic Experts Group). Cette norme, définie par l'ISO, est très utilisée pour la photographie numérique. Elle permet un haut niveau de compression (de l'ordre de 1/40). La contrepartie est une perte de qualité.
Flux audiovisuels	MP3	http://www.mpeg.org		Recommandé, - pérenne, - ouvert, - très utilisé	MP3, abrégé de MPEG-1 Layer III Audio, est une norme de compression du son stéréophonique. MP3 est très répandu. Cette norme intègre cependant des algorithmes brevetés.
	WAV			Possible, - peu pérenne, - propriétaire, - faiblement utilisé	WAV (RIFF WAVE). À l'origine, format de fichier sonore de Microsoft Windows, il est maintenant élargi à d'autres plates-formes. Le son est stéréophonique.
	MPEG-2	http://www.mpeg.org		Recommandé, - pérenne, - ouvert, - très utilisé	MPEG-2 (Moving Picture Expert Group). Cette norme de compression pour les images animées fonctionne sur toutes les plates-formes. Cette norme intègre cependant des algorithmes brevetés.
Flux audiovisuels	MPEG-4	http://www.mpeg.org	ISO/IEC 14496 V2 2000	Recommandé, - pérenne, - ouvert, - utilisé	MPEG-4 est une norme de compression pour les images animées, définie par le Moving Picture Expert Group de l'ISO. Le dernier niveau du standard est aussi nommé H264 par l'UIT. MPEG-4 permet de gérer des flux pour l'accès à travers internet et la visioconférence. DivX, parfois assimilé à tort à MPEG-4, est en fait basé sur MPEG-4 Visual pour l'image et MP3 pour le son.
	DV	http://www.dvformat.com		Possible, - pérenne, - ouvert, - très utilisé	DV (Digital Video cassette) est un format d'acquisition vidéo défini par un consortium de sociétés.
Echange de bases de données	XML	http://www.w3.org/XML		Recommandé, - pérenne, - ouvert, - utilisé	Il est recommandé d'utiliser XML pour les échanges de bases de données.
Echange de bases de données	CSV			Possible, - pérenne, - ouvert, - très utilisé	CSV (Comma Separated Values) Le contenu des bases de données peut être mis sous la forme d'un texte "à plat" doté de séparateurs (virgule de séparation).
Plans	CGM	http://www.iso.ch	IS 8632: 1992	Recommandé, - pérenne, - ouvert, - faiblement utilisé	CGM (Computer Graphics Metafile) est une norme de l'ISO pour la mémorisation et l'échange de données graphiques à deux dimensions.
	STEP	http://www.iso.ch	ISO 10303	Recommandé, - pérenne, - ouvert, - utilisé	STEP (Standard for the Exchange of Product Data). Normes pour l'échange d'informations sur les produits industriels. Ces normes sont répandues.
	DXF			Possible, - pérenne, - propriétaire, - très utilisé	DXF, format propriétaire utilisé par le logiciel Autocad qui est très répandu.

3.1.4 Architectures applicatives

Composant	Version CCI	Standard	RFC	Date / Version	Etat du standard	Commentaires
Protocole d'accès à distance : SOAP	v2	SOAP 1.1	http://www.w3.org/TR/SO	mai-00	Note	
		SOAP 1.2	http://www.w3.org/TR/soap12-part1/ http://www.w3.org/TR/soap12-part2/	déc-02	Recommandé	
Description des services	v2	WSDL	http://www.w3.org/TR/wsdl http://www.w3.org/TR/wsdl12	v1.1 : mars 2001 v1.2 : juin 2003	version 1.1 : Note version 1.2 : Draft	

3.2 TABLEAUX DES STANDARDS « CANDIDATS » ENVISAGES POUR LES VERSIONS ULTERIEURES DU CCI

Les tableaux suivants résument les normes et standards complémentaires candidats au cadre commun d'interopérabilité applicable dans une version Vx à paraître ultérieurement et issu des différentes discussions exposées dans les chapitres précédents.

3.2.1 Interconnectivité

Composant	Standard	RFC	Date / Version	Etat du standard	Commentaires	Référentiels	
LAN/WAN interconnexion	IPv6	RFC 2373	juillet-98	Proposé	Attente de la prise en compte effective par les marchés. Infos IPv6 : http://www.ipv6.org/v6-apps.html		
		RFC 2374	juillet-98	Proposé			
		RFC 2460	décembre-98	Draft			
		RFC 2461	décembre-98	Draft			
		RFC 2462	décembre-98	Draft			
		RFC 2463	décembre-98	Draft			
	Transition IPv -IPv6	RFC 2675			Proposé	Mise à jour V2 : paquets gros volumes	Référentiel Transition IPv6 à prévoir ultérieurement
		RFC 2893	août-00	Proposé			
			RFC 2766	février-00	Proposé		
	FTP		RFC 2428		Proposé	Mise à jour V2 : extensions IPv6	
	DNS		RFC 1886		Proposé		
	DNSSec		RFC 3226		Proposé	Support des enregistrements DNSSec et des adresses IPv6	
			RFC 3445		Proposé	Limitation du champ d'action du Ressource Record KEY	
	TCP		RFC 2018 RFC 2581 RFC 2873 RFC 2883 RFC 3042 RFC 3168 RFC 3390		Proposé Proposé Proposé Proposé Proposé Proposé Proposé	Mise à jour V2 : options proposées	
Wi-Fi		IEEE 802.11g	sept-00	New Std Project	Version émergente		
		IEEE 802.11i	May 2001	En cours	Intègre la sécurité WPA		
Infrastructure de gestion de clés	PKI	RFC 3279	janvier-99	Proposé	Algorithmes et identifiants pour le profile des certificats et des CRL	A prévoir dans un référentiel d'architecture de confiance et description des procédures à respecter.	
		RFC 3280	mars-99	Proposé	Profile des certificats et des CRL		
		RFC 3281	avril-99	Proposé	Profile de certificat d'attribut pour l'autorisation		
Qualité de Service	DiffServ	RFC 2474	décembre-98	Proposé			
		RFC 2597	juin-99	Proposé			
		RFC 2598	juin-99	Proposé			
	RSVP	RFC 2205	septembre-97	Proposé			
		RFC 2680	septembre-99	Proposé			
		RFC 2679	septembre-99	Proposé			
		RFC 2681	septembre-99	Proposé			
Annuaire	X500	RFC 2459, RFC 2510, RFC 2527 et ETSI 101862,			Normes abandonnées au profit de LDAP (à confirmer pour protocole DSP)		
	X 501						
	X 509				Voir Sécurité et PKI		
	Extensions LDAP	RFC 2927	septembre-00	information	cohérence avec le référentiel MAIA		
		RFC 2377	septembre-98	information			
		RFC 2307	mars-98	expérimental			
		RFC 1617	mai-94	information			
Newsgroup	NNTP	RFC 977	février-86	Proposé			

Données

Composant	Version CCI	Standard	RFC	Date / Version	Etat du standard	Commentaires
Metadonnées Metalangage	Vx	ebXML				Les standards ebXML, conjointement développés par UN/CEFACT (UN/Centre for Trade facilitation and Electronic Business) and OASIS (Organization for the Advancement of Structured Information Standards) reprennent une partie de ces concepts du modèle de référence de l'EDI-ouvert (ISO/IEC 14 662). A suivre pour prise en compte ultérieure (lorsque le standard sera industriellement reconnu)
Sécurité XML	Vx	XKMS	N/A	mars-02	Document de travail W3C	Spécifications XKMS 2.0 - http://www.w3.org/TR/xkms2/
	Vx		N/A	mars-02	Document de travail W3C	Exigences XKMS - http://www.w3.org/TR/xkms2-req
	Vx	XACML	N/A	déc-02	Spécifications OASIS	Spécifications XACML - http://www.oasis-open.org/committees/xacml/repository/cs-xacml-specification-01.pdf
	Vx	SAML	N/A	mai-02	Spécifications	Définition du protocole http://www.oasis-open.org/committees/security/docs/cs-sstc-core-01.pdf
	Vx		N/A	mai-02	Spécifications	Règles d'interfaçage avec SAML http://www.oasis-open.org/committees/security/docs/cs-sstc-bindings-01.pdf
	Vx		N/A	mai-02	Spécifications	Considérations relatives à la sécurité et à la protection de la vie privée http://www.oasis-open.org/committees/security/docs/cs-sstc-sec-consider-01.pdf
	Vx		N/A	mai-02	Spécifications	Programme de conformité à SAML http://www.oasis-open.org/committees/security/docs/cs-sstc-conform-01.pdf
Outils de traitement et de présentation des données	Vx	XSL (Extensible Stylesheet Language) XSLT 2.0 XPath 2.0	http://www.w3.org/TR/xslt20/ http://www.w3.org/TR/xpath20/	nov-02	Draft	A suivre pour prise en compte ultérieure (lorsque le standard sera industriellement reconnu)
Modélisation des documents	vx	UMM	http://www.unece.org/cefact/		A prendre en compte en version x	UMM est une méthode d'analyse et de modélisation de processus commerciaux basée sur UML pour le langage et sur RUP pour la méthode

3.2.3 Formats et supports

Composant	Standard	RFC	Date / Version	Etat du standard	Commentaires
Formats de documents	XHTML	http://www.w3.org/TR/xhtml1/		A prendre en compte dans une version ultérieure du CCI	XHTML est une recommandation du World Wide Web Consortium, définie le 26/01/2000 et mise à jour le 01/08/2002. Elle est basée sur XML et définit une syntaxe proche de HTML 4.0 mais plus contrainte.
	OASIS Open Office XML Format	http://www.oasis-open.org/committees/office		A prendre en compte dans une version ultérieure du CCI	OASIS a constitué un groupe de travail pour normaliser un format d'échange de documents basé sur XML, en prenant comme base le format utilisé par OpenOffice.org.
	Microsoft Office v11 XML Format	http://www.microsoft.com/office/developerr/preview/XML.asp		A prendre en compte dans une version ultérieure du CCI	Microsoft annonce pour la version 11 d'Office, une intégration forte de XML. Les composants d'Office pourront lire et produire au format XML. La disponibilité des spécifications d'interface d'Office 11 est un pré-requis pour la prise en compte dans une version ultérieure du CCI.
	PDF/A	http://www.aiim.org/pdf_a		A prendre en compte dans une version ultérieure du CCI	NPES (The Association for Suppliers of Printing, Publishing and Converting Technologies) et AIIM International (Association for Information and Image Management, International) se sont associés pour définir un format d'archivage pérenne, nommé PDF/A et basé sur le format PDF d'Adobe.
	XForms	http://www.w3.org/TR/xforms Candidate Recommendation 20/11/2002		A prendre en compte dans une version ultérieure du CCI	XForms est une recommandation candidate du World Wide Web Consortium, définie le 20/11/2002. Elle est basée sur XML et permet la réalisation de formulaires. XForms gère séparément la présentation et le contenu. XForms permet le typage des données à saisir. Cette norme n'est pas un nouveau type de document, mais est conçue pour être intégrée dans des langages comme XHTML ou SVG.
Images fixes	SVG	http://www.w3.org/TR/svg Recommendation v1.0 04/09/2001		A prendre en compte dans une version ultérieure du CCI	SVG 1.0 (Scalable Vector Graphic) est une norme du World Wide Web Consortium, définie le 04/09/2001. Elle est basée sur XML et permet la description d'objets graphiques vectoriels en deux dimensions. Elle permet l'interactivité, le scripting et l'animation.
Flux de données audio	Ogg Vorbis	http://www.vorbis.com http://vorbismusic.free.fr v1.0		A prendre en compte dans une version ultérieure du CCI	Ogg Vorbis est une technologie d'encodage, de lecture et de diffusion audio, distribuée en logiciel libre, sous licence GPL. Ogg Vorbis a pour objectif de remplacer le format MP3.
Echange de données audiovisuelles	AAF	http://www.aafassociation.org		A prendre en compte dans une version ultérieure du CCI	AAF (Advanced Authoring Format/ Format d'édition avancé), a été développé par Avid et est proposé en format logiciel libre depuis 2000. AAF permet l'échange de données multimédias composites entre producteurs multimédia.
	MPEG-4 part 10 / H.26L			Cette norme, en cours de définition, est proposée pour une version ultérieure du CCI.	ISO/MPEG et l'UIT élaborent actuellement MPEG-4 part 10 / H.26L, avec l'objectif d'une norme ne comprenant pas de versement de redevances (<i>royalty-free</i>).

3.2.4 Architectures applicatives

Composant	Version CCI	Standard	RFC	Date / Version	Etat du standard	Commentaires
Sécurité WS	Vx	WS-Security	N/A	déc-02	Document de travail	Spécifications WS Security http://www.oasis-open.org/committees/wss/documents/WSS-Core-08-1212-merged.pdf
	Vx		N/A	sept-02	Document de travail	Support de Kerberos http://www.oasis-open.org/committees/wss/documents/WSS-Kerberos.pdf
	Vx		N/A	déc-02	Document de travail	Support de SAML http://www.oasis-open.org/committees/wss/documents/WSS-SAML-05.pdf
	Vx		N/A	sept-02	Document de travail	Support des certificats X.509 http://www.oasis-open.org/committees/wss/documents/WSS-X509.pdf
	Vx		N/A	sept-02	Document de travail	Support de XrML http://www.oasis-open.org/committees/wss/documents/WSS-XrML-01.pdf
	Vx		N/A	nov-02	Document de travail	Support de XCBF http://www.oasis-open.org/committees/wss/documents/WSS-XCBF.pdf
Description de répertoire des services	Vx	UDDI	http://www.uddi.org/	v2 : juillet 2003 v3 : juillet 2003		A suivre pour prise en compte ultérieure