Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

**Ministère délégué au budget et à la réforme de l'Etat**

**Direction Générale de la Modernisation de l'Etat**

# Référentiel Général d'Interopérabilité

## Interopérabilité Technique

## Normes et recommandations

# Références documentaires

<1> Ordonnance n°2005-1516 sur les échanges électr oniques du 8 décembre 2005, (Journal Officiel du 9 décembre 2005).

<2> Introduction au Référentiel Général d'Interopérabilité. V1.4 du 26-02-2006.

<3> Référentiel Général d'Interopérabilité. Glossaire.

<4> Schéma Directeur Adèle.

# Sommaire

# Table des Règles d'Interopérabilité Technique

Numéro de page



Numéro de page

# 1 - Présentation générale et guide d'usage

## 1.1 - Présentation

L'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives elle-même, s'inscrit dans la démarche globale du Gouvernement de réforme de l'Etat, plus précisément dans ses aspects de simplification des démarches des usagers et de facilitation de l'accès de ces derniers aux services publics.

Cette ordonnance introduit la notion de Référentiel Général d'Interopérabilité (RGI) dont l'objet est de fixer les règles techniques permettant d'assurer l'interopérabilité de tout ensemble de moyens destinés à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives.

Une des composantes du RGI concerne l'interopérabilité technique, ensemble de normes et de standards qui doivent être utilisés par les autorités administratives et dont le respect conditionne le développement de l'offre de services administratifs accessibles par voie électronique.

L'objectif du présent document est de traiter cette composante et de cibler plus particulièrement les chefs de projet, architectes et développeurs travaillant sur des projets relatifs à l'administration électronique. Afin de renforcer son caractère opérationnel, il se matérialise sous la forme d'un ensemble de règles d'interopérabilité qui précise les normes, standards, recommandations, principes de mise en œuvre et composants à utiliser.

Ce document respecte les conditions d'élaboration, d'approbation, de modification et de publication fixées par décret.

En application du principe de subsidiarité, ces règles ne s'appliquent qu'aux problématiques d'échange (pris au sens large) entre les usagers et l'administration ainsi qu'entre les différentes autorités administratives. Pour leurs besoins internes, les administrations et les collectivités territoriales restent libres du choix des normes, principes et composants à utiliser.

## 1.2 - Niveau de préconisation

Les règles présentées dans ce document ont différents niveaux de préconisation inspirés de la RFC 2119[1] :

- **OBLIGATOIRE :** ce niveau de préconisation signifie que la règle édictée indique une exigence absolue du RGI.
- **RECOMMANDÉ :** ce niveau de préconisation signifie qu'il peut exister des raisons valables, dans des circonstances particulières, pour ignorer la règle édictée, mais les conséquences doivent être comprises et pesées soigneusement avant de choisir une voie différente.
- **DÉCONSEILLÉ :** ce niveau de préconisation signifie que la règle édictée indique une prohibition qu'il est toutefois possible, dans des circonstances particulières, de ne pas suivre, mais les conséquences doivent être comprises et le cas soigneusement pesé.
- **INTERDIT :** ce niveau de préconisation signifie que la règle édictée indique une prohibition absolue du RGI.

**Remarque :** il n'existe pas de niveau de préconisation «POSSIBLE» car le RGI se veut être un référentiel de recommandations à appliquer et pas un état de l'art de ce qu'il est possible de faire.

[1] http://www.ietf.org/rfc/rfc2119.txt

Toute équipe de développement interne ou externe devra spécifier et justifier les points suivants :

- les circonstances et justifications de non respect d'une règle RECOMMANDÉE,
- les circonstances et justifications de non respect d'une règle DÉCONSEILLÉE,
- les justifications des exceptions à toute règle absolue (OBLIGATOIRE ou INTERDIT) ; et dans ce dernier cas, l'avis de la DGME doit être demandé au préalable et joint au dossier.

## 1.3 - Gestion du document

Le présent document est sous la responsabilité de la DGME qui est chargée de respecter les conditions d'élaboration, d'approbation, de modification et de publication fixées par décret, ce qui se traduit notamment par :

- La publication sur le site de la DGME afin qu'il soit consultable par tous,
- La mise à jour régulière afin de tenir en compte des évolutions des technologies et des usages des autorités administratives soumises à l'application de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

# 2 - Présentation détaillée

## 2.1 - Composition d'une fiche

Un thème regroupe un certain nombre de règles d'interopérabilité par affinité d'intérêt pour un chef de projet ou un architecte.

Chaque fiche thématique contient les éléments suivants :

- **Description :** présentation de l'objectif du thème et des métadonnées associées (nom du responsable de la fiche, catégories de classification, etc.).
- **Normes et Standards :** éléments définis par des organismes de normalisation (par exemple : JPEG, HTML, etc.). C'est sur ces éléments que s'appuient les règles énoncées.
- **Principes de mise en œuvre :** profils d'utilisation ou principes opérationnels d'architecture (par exemple : profil de messagerie, modèles d'architecture de fédération d'identité, modèles d'intégration des téléservices aux portails, etc.).
- **Composants :** il s'agit d'éléments mutualisés ou réutilisables (par exemple : un service de validation d'adresse géopostale, un service ICG, un produit Open Source, etc.).
- **Procédures de vérification de conformité :** (dans les cas complexes pertinents) séquences, points de contrôle, procédures de recettes instrumentées permettant de vérifier la conformité aux règles.
- **Pratiques sectorielles :** références de pratiques, normes et standards que certains secteurs (exemples : fiscal, social, juridique, transport, marché public, etc.) mettent en œuvre.

## 2.2 - Présentation des règles

Les règles sont présentées de la manière suivante dans la suite du document.

| | |
|---|---|
| Champ1 | *Libellé de la règle. Libellé de la règle. Libellé de la règle.* |

Le champ1 décrit le volet concerné et le numéro d'ordre de la règle dans ce volet. Les valeurs possibles sont RITn, RISn, RIOn, etc.

RIT = Règle d'Interopérabilité Technique.

RIS = Règle d'Interopérabilité Sémantique.

RIO = Règle d'Interopérabilité Organisationnelle.

Le paramètre n est incrémenté à partir de 1 sans souci de hiérarchisation.

Le libellé de la règle est un texte libre en formulation et en longueur. Il doit toutefois commencer par une des formules suivantes : «Il est OBLIGATOIRE», «Il est RECOMMANDÉ», «Il est DÉCONSEILLÉ», «Il est INTERDIT».

# 3 - Interopérabilité des formats de données

## 3.1 - Codage des caractères

### 3.1.1 - Description

| | |
|---|---|
| **Objectif** | Ces règles permettent de définir le codage des caractères utilisés pour les échanges entre les administrations et les usagers et de garantir ainsi l'interopérabilité. |
| **Domaine d'interopérabilité** | Tous les services d'administration électronique. |
| **Responsable** | |

### 3.1.2 - Le codage des caractères sur un octet

| | |
|---|---|
| RIT0001 | Il est OBLIGATOIRE d'utiliser la norme ISO 8859-15 Latin 9, pour l'encodage sur un octet des caractères. |

Le code **ASCII** (*American Standard Code for Information Interchange*), a été inventé en 1961 pour le codage des caractères alphanumériques en informatique. Il utilise les 7 bits de poids faible d'un octet ce qui permet de définir 128 caractères. Le bit de poids fort est à 0. A ce jour le code ASCII est encore souvent utilisé, même si parfois complété par une table étendue. En effet, de nombreuses pages de codes étendent l'ASCII en utilisant le bit de poids fort pour définir des caractères supplémentaires (numérotés de 128 à 255).

C'est ainsi que la norme **ISO 8859** fournit des extensions pour diverses langues. Par exemple, la norme ISO 8859-1, appelée aussi « Latin-1 », étend le code ASCII avec les caractères accentués utiles aux langues d'Europe de l'ouest. Toutefois, cette norme a évolué car elle contenait des erreurs.

Le jeu de caractères ISO-8859-15 (Latin 9) corrige et remplace le jeu de caractères Latin 1. Il introduit également le caractère € de l'euro. Ce jeu est supporté par les principaux navigateurs web disponibles.

Par ailleurs, une nouvelle partie de la norme ISO vient d'être publiée. Il s'agit de la norme ISO-8859-16 (Latin 10). Cette partie étant très récente, nous nous prononcerons sur son introduction dans une règle du RGI ultérieurement.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| ISO/IEC 8859-15:1999 | Jeux de caractères graphiques codés sur un seul octet -- Partie 15 : Alphabet latin n°9<br>http://www.iso.org/iso/fr/CatalogueDetailPage.CatalogueDetail?CSNUMBER=29505&ICS1=35&ICS2=40&ICS3= | Norme publiée | Jan 2005 |
| ISO/IEC 8859-16:2001 | Jeux de caractères graphiques codés sur un seul octet -- Partie 16 : Alphabet latin no 10<br>http://www.iso.org/iso/fr/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33428&ICS1=35&ICS2=40&ICS3= | Norme publiée | 1er mars 2006 |

### 3.1.3 - Le codage des caractères sur plusieurs octets

| | |
|---|---|
| RIT0002 | Il est OBLIGATOIRE d'utiliser UNICODE v4.1.0, pour l'encodage multi-octets des caractères. |

Le jeu de caractères ASCII n'est pas suffisant pour un système d'information global tel que le World Wide Web, c'est pourquoi HTML utilise le jeu de caractères bien plus important, appelé jeu de caractères universel codés sur plusieurs octets (UCS Universal Character Set), défini par la norme ISO 10646, et par la recommandation du consortium UNICODE.

La norme **ISO 10646** s'applique à la représentation, à la transmission, à l'échange, au traitement, au stockage, à la saisie et à la présentation des langues du monde sous forme écrite et de symboles complémentaires. Elle a permis d'unifier les différents codages de caractères complétant le code ASCII, et d'y intégrer des codages complètement différents comme par exemple le code JIS pour le Japonais.

La version 4.1.0 de la recommandation UNICODE définit un ensemble de caractères, de noms et de représentations codées identiques, caractère par caractère, à l'ensemble de l'ISO/IEC 10646:2003. Elle fournit, de surcroît, des informations supplémentaires relatives aux propriétés de ces caractères, aux algorithmes de traitement ainsi que des définitions utiles aux développeurs.

La norme ISO 10646:2003 a été adoptée par de nouveaux protocoles Internet et mise en oeuvre dans des systèmes d'exploitation et des langages informatiques. Elle contient plus de 95.000 caractères des écritures utilisées par les communautés du monde entier.

**Ceci favorise l'interopérabilité et l'échange de données au niveau international. Ce codage est donc à recommander dans un contexte d'échanges internationaux.**

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| ISO/IEC 10646:2003 | Jeu Universel de Caractères codés sur plusieurs octets. http://www.iso.org/iso/fr/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39921&ICS1=35&ICS2=40&ICS3= | Norme publiée | Déc 2003 |
| UNICODE v4.1.0 | http://www.unicode.org/versions/Unicode4.1.0/ | Recommandé | Mars 2005 |
| UNICODE v5.0.0 | http://www.unicode.org/versions/Unicode5.0.0/ | En beta-test | 3ème trim. 2006 |

Il est important de noter que la recommandation UNICODE est exigée par de nombreux standards récents tels que XML, Java, ECMAScript, LDAP, CORBA 3.0, WML, etc.

Une liste partielle de produits supportant la recommandation UNICODE est disponible à l'adresse suivante :

http://www.unicode.org/onlinedat/products.html

### 3.1.4 - Le codage UTF des caractères

UTF-8 (*UCS transformation format* 8 bits) est un format de codage de caractères défini pour les caractères UNICODE. C'est une extension du code ASCII utilisant le bit de poids fort. Chaque caractère est codé sur une suite de un à quatre octets (cette taille variable est un inconvénient). Il a été conçu pour être compatible avec certains logiciels originellement prévus pour traiter des caractères d'un seul octet.

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

L'IETF requiert qu'UTF-8 soit supporté par les protocoles de communication d'Internet échangeant du texte. Le format UTF-8 est en effet le format de codage que tous les sites web utiliseront à terme car il permet de couvrir le codage de toutes les lettres et symboles de tous les langages. L'utilisation du format UTF-8 faciliterait donc à la fois la maintenance et l'accessibilité des sites web. Les principaux navigateurs du marché prennent en charge le standard UTF-8 depuis 1998.

UNICODE et ISO 10646 acceptent d'autres formes de transformation universelle comme UTF-16 et UTF-32. Mais nous ne développerons pas ce sujet dans ce document.

**Compte tenu de tout cela, le format UTF-8 doit donc être mentionné dans le présent document. Il sera nécessaire de se prononcer sur l'utilisation du format UTF-8 par rapport à tout autre format, y compris le format ISO-8859-15.**

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| RFC 3629 | UTF-8 un format de transformation d'ISO 10646<br><br>http://www.ietf.org/rfc/rfc3629.txt | Standard | Nov 2003 |

## 3.2 - Formats des images fixes

### 3.2.1 - Description

| | |
|---|---|
| **Objectif** | Ces règles permettent de définir les formats d'échange d'images fixes de tous types entre les administrations et les usagers et de garantir ainsi l'interopérabilité. |
| **Domaine d'interopérabilité** | Accès aux services en ligne. |
| **Responsable** | |

### 3.2.2 - Normes et standards Images fixes

| | |
|---|---|
| RIT0003 | Il est OBLIGATOIRE d'utiliser le format PNG v1.2 pour les échanges d'illustrations non photographiques (par exemple : schéma, icône ou logo). |
| RIT0004 | Il est RECOMMANDÉ d'utiliser le format PNG v1.2 pour la présentation (affichage) d'illustrations non photographiques. |

Le format PNG (Portable Network Graphics) vise à remplacer le format propriétaire GIF pour la compression sans pertes. Ce format est promu par l'association W3C et par l'ISO.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| PNG v1.2 | http://www.libpng.org/pub/png/<br><br>http://www.w3.org/TR/PNG | En appel à commentaire | 10 nov 2003 |
| ISO/IEC 15948:2004 | Infographie et traitement d'images -- Graphiques de réseau portables (PNG): Spécification fonctionnelle. | Norme publiée | 3 mar 2004 |

Principes : PNG 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. En effet, le format GIF est la propriété de la société Unisys, également propriétaire de l'algorithme de compression LZW, ce qui oblige chaque éditeur de logiciel manipulant ce type de format à verser des droits.

PNG propose donc un format ouvert et non propriétaire, basé sur une version publique de LZW.

Caractéristiques techniques : Le format PNG supporte tous les styles d'images Bitmap : les images Noir et Blanc, les images en True Color (couleurs réelles), les images aux couleurs indexées. Il peut gérer une couche Alpha de transparence, c'est-à-dire que n'importe quelle couleur peut être en partie transparente, comme un calque dans Photoshop ou les icônes en True Color pour Windows XP. Il peut intégrer le codage de la correction Gamma et des méta-données.

http://www.iso.org/iso/fr/CatalogueDetailPage.CatalogueDetail?CSNUMBER=29581&ICS1=35&ICS2=140&ICS3=

Comme le format GIF, le PNG possède aussi une fonction d'entrelacement permettant d'afficher l'image progressivement, ce qui accélère la chargement d'une page Web, par exemple. La compression proposée par ce format est une compression sans perte, de 5 à 25% meilleure que la compression GIF.

Utilisation préférentielle

Petites images graphiques, par exemples des logos, des dessins, des schémas.

Malheureusement, le PNG est encore peu utilisé : les navigateurs ne l'interprètent pas toujours bien, et ne tirent pas encore profit de toutes ses possibilités (couche alpha, gamma, etc.). De plus les logiciels d'optimisation d'images pour le web, Image Ready et Fireworks, ne l'utilisent pas de la même façon : seul Fireworks, dont il est le format natif, semble en tirer pleinement profit et le compresse mieux qu'un GIF.

### 3.2.3 - Normes et standards Images fixes (autre format)

| | |
|---|---|
| RIT0005 | Il est DÉCONSEILLÉ d'utiliser le format GIF pour la présentation (affichage) d'illustrations non photographiques (par exemple : schéma, icône ou logo). |

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| GIF<br>Version 89a | http://www.w3.org/Graphics/GIF/spec-gif89a.txt | Format publié mais propriétaire | 31 juil 1990 |

Principes

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, appelé LZW (brevets Unisys), utilisé par les fichiers ZIP et qui est aussi une option du format TIFF. C'est un encodage de redondance de code en longueur de ligne, de la droite vers la gauche : ainsi toute surface régulière horizontale (aplat de couleur) est très fortement compressée. GIF sait gérer des zones transparentes, une des couleurs de sa palette est transparente : cette fonction permet de positionner un objet détouré sur le fond de la page web. GIF a une option d'entrelacement équivalente au JPEG progressif, avec les mêmes avantages et inconvénients.

Le format GIF est utilisé sur le Web pour les images synthétiques, tandis que JPEG est utilisé pour les photographies et que Macromedia Flash tend à s'imposer pour les animations.

Il est à noter que le dernier brevet d'Unisys sur ce sujet est arrivé à expiration en juillet 2004. Par contre IBM détient encore un brevet valide jusqu'en août 2006 aux USA (et peut-être après dans d'autres pays).

## 3.2.4 - Normes et standards Illustrations photographiques

| | |
|---|---|
| RIT0006 | Il est RECOMMANDÉ d'utiliser la norme JPEG (ISO 10918) pour l'échange et la présentation d'illustrations photographiques. |

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 (de l'ordre de 1/40) 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.

Utilisation préférentielle

Reproduction de photographies de grande taille, avec de nombreuses couleurs (son usage devient intéressant à partir d'une taille de 100x100 pixels).

Avantages : forte compression des données, peu d'espace mémoire requise pour le stockage, rapidité de transmission sur les réseaux.

Inconvénients : perte de qualité si le taux de compression est trop élevé, altération de données vectorielles pixelisées (textes, dessins), nécessite de la mémoire et de la puissance processeur pour la décompression des fichiers.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| JPEG | ISO/IEC 10918-4:1999<br>Compression numérique et codage des images fixes de nature photographique. | Norme publiée | 1999 |
| | ITU-T Recommendation T.81<br><br>http://www.itu.int/ITU-T/ | Norme approuvée<br>Corrigée en 2004 | 1992<br>janv 2004 |
| | ITU-T Recommendation T.851 | Norme approuvée | Sept 2005 |
| | http://www.jpeg.org | | |

La norme JPEG2000 est le nouveau système de codage d'image utilisant l'état de l'art actuel des technologies de compression et basé sur la transformée en ondelettes. Son architecture devrait être appropriée à un grand nombre d'applications depuis les appareils photos digitaux jusqu'à l'imagerie médicale et d'autres secteurs clé. La compression est avec ou sans perte d'information.

La partie 1 définit le noyau de la norme. Celui-ci comprend la syntaxe du codestream JPEG 2000 ainsi que les étapes nécessaires pour coder et décoder des images. Les parties ultérieures de la norme concernent différents types d'extensions, dont aucune n'est essentielle à l'implémentation basique. Certaines implémentations existantes n'utilisent que la Partie 1.

JPEG 2000 a été développé avec l'objectif de permettre l'implémentation de la Partie 1 sans devoir payer de royalties ou de frais de licence, et des propriétaires de brevets ont renoncé à leurs droits pour atteindre cet objectif. Cependant, le comité JPEG ne peut faire de garantie formelle, et c'est le responsable de l'implémentation qui a la charge de s'assurer qu'aucun brevet n'est violé.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| JPEG 2000 | ISO/IEC 15444-1:2004<br>Système de codage d'image JPEG 2000 | Norme publiée | Sept 2004 |
| | ITU-T Recommendation T.800<br>http://www.itu.int/ITU-T/ | Norme approuvée | Août 2002 |
| | ITU-T Recommendation T.800 (2002)<br>Amendment 1 | Norme approuvée | Sept 2005 |
| | http://www.jpeg.org/jpeg2000/index.html?langsel=fr | | |

## 3.2.5 - Normes et standards Images fixes non compressées

| | |
|---|---|
| RIT0007 | Il est OBLIGATOIRE d'utiliser le format TIFF v6.0 pour les échanges d'images qui ne doivent pas être compressées. |
| RIT0008 | Il est INTERDIT d'utiliser le format TIFF v6.0 pour la présentation d'images puisqu'il n'existe pas en standard de logiciel de lecture. |

Principes

Le *Tag(ged) Image File Format* généralement abrégé en TIFF est un format de fichier pour image numérique fixe. Il a été développé par les sociétés Microsoft et Aldus. La société Adobe-Systems a acheté Aldus et possède donc maintenant les droits sur le texte de la spécification TIFF et la marque TIFF.

C'est un format extrêmement flexible, ce qui fait qu'il est utilisé dans des applications très diverses, des scanners industriels et télécopieurs aux appareils photo numériques en passant par les imprimantes. En revanche cette grande souplesse fait qu'il n'existe pas de logiciel capable d'afficher n'importe quelle image TIFF.

Par ailleurs, TIFF utilise des types de compression permettant de garantir la qualité et l'absence de perte d'information.

Utilisation préférentielle

Les documents à compresser sans perte de qualité. Ce sont principalement les documents administratifs et les documents provenant de numérisation de formulaires renseignés de façon manuscrite.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| TIFF v6.0 | http://partners.adobe.com/public/developer/en/tiff/TIFF6.pdf | Format publié mais propriétaire | Juin 1992<br>Mars 1995 |

## 3.2.6 - Formats d'images déconseillés

| | |
|---|---|
| RIT0009 | Il est DÉCONSEILLÉ d'utiliser les formats EPS, PICT, BMP, PCX pour l'échange et la présentation d'images. |

**EPS (Encapsulated PostScript)** : Ce format utilisé par de nombreux programmes de dessin et de mise en page. Elaboré pour le monde de la pré-presse, il offre de nombreuses possibilités : fichier Tiff de prévisualisation pour la mise en page, possibilité de compresser en JPEG les couches CMJN en un seul fichier ou en quatre fichiers distincts. EPS est sans doute le format le plus ouvert puisqu'il est capable de décrire à la fois des images vectorielles et Bitmap, ainsi que les données de la mise en page. C'est un format lourd puisqu'il contient beaucoup d'informations. Il s'intègre parfaitement au monde de la PAO car Il génère une image de prévisualisation Tiff basse résolution pour faciliter la mise en page dans X PRESS ou Page Maker.

**PICT** est un format utilisé pour le transfert d'image entres les applications Macintosh de dessin vectoriel et de mise en page. Choix de l'échantillonnage de 8, 16 ou 32 bits par pixel.

**BMP** acronyme de Bitmap, est un format d'image numérique ouvert développé par Microsoft et IBM. C'est un des formats d'images les plus simples à développer et à utiliser pour programmer. Il est lisible par quasiment tous les visualiseurs et éditeurs d'images. Le format BMP est quasiment inexistant sur le Web : il ne dégrade pas l'image et n'utilise généralement pas de compression, aussi est-il très lourd. Il existe néammoins la compression RLE pour le format BMP.

Le **PCX** est un format d'image numérique dont l'encodage est basé sur une forme de *run-length encoding*. PCX a été développé par la société ZSoft Corporation. C'était le format de base de leur logiciel *PC Paintbrush*, un des logiciels d'édition d'images les plus populaires sous le système d 'exploitation DOS. La plupart des fichiers PCX utilisent une palette de couleurs, mais le format a été étendu pour permettre l'utilisation d'images 24 bits et dans ce cas l'encodage est réalisé en séparant les trois composantes de couleur. Le format PCX était très populaire sur les premiers systèmes DOS et Windows, mais il se fait de plus en plus rare, car il existe de nos jours des formats permettant une compression bien meilleure, comme par exemple GIF, JPEG et PNG.

## 3.2.7 - Formats d'images à débattre

**SVG (Scalable Vector Graphic)** est un standard du World Wide Web Consortium, défini en 2001. Il est basé sur XML et permet la description d'objets graphiques vectoriels en deux dimensions. Il permet l'interactivité, le scripting et l'animation.

Malgré toutes ses qualités, ce format est faiblement diffusé.

## 3.3 - Formats des images animées

### 3.3.1 - Description

| | |
|---|---|
| **Objectif** | Ces règles permettent de définir les formats d'échange d'images animées entre les administrations et les usagers et de garantir ainsi l'interopérabilité. |
| **Domaine d'interopérabilité** | Accès aux services en ligne |
| **Responsable** | |

### 3.3.2 - Normes et standards Animation simple d'images

| | |
|---|---|
| RIT0010 | Il est RECOMMANDÉ d'utiliser le format « GIF animé » pour les animations graphiques simples et/ou de courte durée. |

Principe

GIF animé (Graphic Interchange Format) est un format répandu. En 1989, le format GIF pour image fixe a été étendu (format GIF89a au lieu de GIF87a) pour permettre le stockage de plusieurs images dans un même fichier et pour définir leur séquencement. 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.

Utilisation préférentielle

Utilisation : Graphiques, dessins, logos, textes, petites images (les défauts dus à la réduction en 256 couleurs étant alors peu visibles, les faibles taux de compression du LZW sont moins critiques sur de petites images), logos animés, logos non rectangulaires.

Limitation : convient mal aux images photographiques complexes (LZW les compresse mal, la réduction en 256 couleurs crée des défauts trop visibles) et en général aux images de grande taille.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| GIF<br>Version 89a | http://www.w3.org/Graphics/GIF/spec-gif89a.txt | Format publié mais propriétaire | 31 juil 1990 |

### 3.3.3 - Normes et standards Animation simple d’images

Le format MNG, Multiple-image Network Graphics, est un format de fichier ouvert de droit, permettant de réaliser des images animées. Il est étroitement lié au format d'image PNG.

Plusieurs navigateurs Web affichent déjà MNG; et des plugins de MNG sont disponibles pour Mozilla et Internet Explorer. Les concepteurs de MNG espèrent que ce format remplacera à terme le GIF pour des images animées sur le Web, de la même façon que le format PNG a déjà commencé à le faire pour des images fixes. Toutefois, MNG n’est pas aussi largement soutenu que le PNG.

La structure des fichiers au format MNG est identique à celle des fichiers PNG, différant seulement dans la signature et dans l'utilisation d’unités d’information discrètes. Les images utilisées dans l'animation sont stockées dans le fichier MNG comme une encapsulation d’images au format PNG ou JNG.

Deux versions de MNG de complexité réduite ont été également créées : MNG-LC (faible complexité) et MNG-VLC (complexité très faible). Celles-ci permettent à des applications d'inclure le support de MNG à un certain degré, sans devoir mettre toutes les spécifications de MNG.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| MNG | http://www.libpng.org/pub/mng/ | En appel à commentaire | Jan 2001 |

## 3.3.4 - Normes et standards Animation complexe d'images

| | |
|---|---|
| RIT0011 | Il est RECOMMANDÉ d'utiliser le format Flash v7.2 ou le format Flash v8 pour les animations graphiques complexes et/ou de plus longue durée. |

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 Abode Systems en décembre 2005.

**Il ne doit pas être utilisé pour réaliser des interfaces. Sur ce sujet, se reporter au chapitre « Recommandations sur les IHMs ».**

L'inconvénient pour les utilisateurs de Flash est la nécessité de la présence d'un composant (appelé plug-in) sur le navigateur du poste de travail de l'internaute. Ce composant existe désormais sur de nombreuses plateformes et systèmes d'exploitation. Le lecteur Flash ou le plug-in serait présent sur 97% des navigateurs du monde entier. Le composant Flash Player est un plug-in propriétaire et dont les sources ne sont pas disponibles.

L'extension d'un fichier au format Flash est « **.swf** ».

Cependant, la publication en octobre 1998 des spécifications du format Flash (SWF) version 3 a rendu plus simple le développement d'applications compatibles avec Flash. À l'heure actuelle, de très nombreux logiciels, tel que OpenOffice.org, peuvent exporter dans ce format. Toutefois une partie des technologies utilisées dans le lecteur ou le plug-in Flash restent non publiques ou sujettes à brevet (compression audio et vidéo par exemple).

La technologie Flash étant de plus en plus utilisée pour du contenu publicitaire, parfois intempestif, il a été créé pour Mozilla et ses dérivés des extensions comme FlashBlock permettant de bloquer le contenu Flash publicitaire, le chargement de pages d'introduction non désirées et les requêtes d'installation de Flash.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| Flash v7.2<br>Flash v8 | http://www.macromedia.com | Propriétaire | 2004<br>2005 |

Par ailleurs, il existe une communauté Open Source autour du format Flash. Ses travaux sont consultables à l'adresse suivante :

http://osflash.org/

Cette information est donnée à titre de veille technologique et peut être une base de réflexion pour une future version de ce document.

## 3.4 - Formats pour le son et la vidéo

### 3.4.1 - Séquences sonores

| | |
|---|---|
| RIT0012 | Il est RECOMMANDÉ d'utiliser la norme MPEG-1/2 Audio Layer 3 (dite MP3) pour diffuser et sauvegarder des séquences sonores. |

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.

L'extension d'un fichier audio compressé au format MPEG-1/2 Audio Layer 3 est « **.mp3 »**.

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).

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| MP3 | ISO/IEC IS 11172-3<br>Codage de l'image animée et du son associé pour les supports de stockage numérique jusqu'à environ 1,5 Mbit/s. Partie 3 : Audio. | Norme publiée | 1993 |
| | ISO/IEC IS 13818-3<br>Codage générique des images animées et des informations sonores associées. Partie 3 : Son. | Norme publiée | 1998 |
| | http://www.mpeg.org<br><br>http://www.chiariglione.org/mpeg/ | | |

### 3.4.2 - Formats sonores déconseillés

| | |
|---|---|
| RIT0013 | Il est DÉCONSEILLÉ d'utiliser le format WAV pour sauvegarder des séquences sonores à des fins d'archivage. |

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.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| WAV | http://quimby.gnus.org/internet-drafts/draft-ema-vpim-wav-00.txt | « Internet Draft »<br>Format propriétaire | Juin 1999 |

| | |
|---|---|
| RIT0014 | Il est DÉCONSEILLÉ d'utiliser le format WMA pour diffuser et sauvegarder des séquences sonores. |

Le format Windows Media Audio aussi appelé WMA est un format de compression audio développé par la société Microsoft. Il permet, comme le MP3, de stocker de grandes quantités de sons (musique, voix) grâce à une compression des données. Le WMA gère deux types de compression, la Compression avec perte (lossy) et la Compression sans perte (Lossless).

L'arrivée en 2003 du Codec version 9, a introduit plusieurs versions du format WMA :

Compression avec pertes de la musique,
Format spécialisé dans la reproduction de la voix,
Compression du son en haute définition,
Compression non destructrice de la musique.

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.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| WMA | http://www.microsoft.com | Format propriétaire | 1999 |

### 3.4.3 - Autre format sonore émergeant

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.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| OGG Vorbis V1.0 | http://www.vorbis.com/ | | Juil 2002 |

### 3.4.4 - Séquences vidéo

| | |
|---|---|
| RIT0015 | Il est OBLIGATOIRE d'utiliser la norme ISO 13818 (MPEG-2) pour la présentation de séquences vidéo basse définition. |
| RIT0016 | Il est RECOMMANDÉ d'utiliser la norme ISO 13818 (MPEG-2) pour les échanges de séquences vidéo basse définition. |

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.

La norme ISO/IEC 13818-1 (Codage générique des images animées et du son associé – Partie Système) définit les aspects Systèmes (synchronisation, transport, stockage).

Les normes ISO/IEC 13818-2 et 3 (Codage générique des images animées et du son associé - Parties vidéo et audio) définissent les aspects compression du signal.

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).

| **Nom + Version** | **Spécification** | **Etat** | **Date** |
|---|---|---|---|
| MPEG-2 | ISO/IEC IS 13818<br>Codage générique des images animées et des informations sonores associées. | Norme publiée et révisée périodiquement | 1994 |
| | ITU Recommandation H.262<br>Codage générique des images animées et du son associé. Données vidéo.<br><br>http://www.itu.int/ITU-T/ | Norme publiée et révisée périodiquement | 1995 |
| | http://www.mpeg.org<br><br>http://www.chiariglione.org/mpeg/ | | |

## 3.5 - Formats pour l’audiovisuel et la vidéo HD

### 3.5.1 - Description

| | |
|---|---|
| **Objectif** | Ces règles visent à garantir l'interopérabilité entre les différents services techniques des administrations. Cela permet à une administration d'utiliser ou d'intégrer dans ses propres applications des services techniques mis à disposition par d'autres administrations, par exemple, accéder à un service d’annuaire, transporter des données ou échanger des fichiers. |
| **Domaine d’interopérabilité** | Intégration entre services techniques<br>Services audiovisuels<br>Vidéoconférence, visiophonie<br>Vidéo Haute Définition |
| **Responsable** | |

### 3.5.2 - La norme MPEG4

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

MPEG-4 est d'abord conçu pour gérer le contenu de scènes comprenant un ou plusieurs objets audio-vidéo. Contrairement à MPEG-2 qui visait uniquement des usages liés à la télévision numérique (diffusion DVB et DVD), les usages de MPEG-4 englobent toutes les nouvelles applications multimédias comme le téléchargement et le *streaming* sur Internet, le multimédia sur mobile, la radio numérique, les jeux vidéo, la télévision et les supports haute définition.

MPEG-4 a développé de nouveaux codecs audio et vidéo et enrichie les contenu multimédia, en ajoutant de nouvelles comme VRML (étendu), support pour des présentation 3D, des fichiers composite orienté-objet (incluant des objets audio, vidéo et VRML), le support pour la gestion des droits numériques et plusieurs types d'interactivités.

MPEG-4 se décompose en une suite de normes, les parties, qui spécifient un type de codage particulier. Dans chaque partie plusieurs profils (collection d'algorithmes) et niveaux (contraintes quantitatives) sont définis. Un consortium industriel désirant utiliser MPEG-4 choisit une ou plusieurs parties de la norme et, pour chaque partie, il peut sélectionner un ou plusieurs profils et niveaux correspondant à ses besoins.

Le format DivX est quant à lui basé sur MPEG-4 Visual pour le codage de l'image et sur MP3 pour le codage du son.

### 3.5.3 - La recommandation H.264

Le dernier niveau du standard MPEG4 est aussi nommé H.264 par l'UIT.

H.264 est un codec de compresion vidéo numérique des images et vidéo haute définition à la norme MPEG-4, développé par le VCRG (Video Coding Experts Group) en partenariat avec le MPEG (Moving Picture Experts Group), aussi connu sous l'appellation AVC (Advanced Video Coding). Le projet H.264/AVC a permis de créer un standard de fourniture de vidéo de qualité avec un 'bit rate' sensiblement inférieur (minimum de moitié) aux précédents standards, sans en augmenter la complexité afin de conserver un niveau de design raisonnable pour un spectre de résolution élargi.

Ce nouveau codec de compression vidéo est une évolution logique du MPEG4. La recommandation H264 devrait améliorer le taux de compression tout en proposant une meilleure qualité d'affichage. Elle devrait ainsi offrir un taux de compression de 2 à 3 fois plus élevé que le MPEG-2 et de 1.5 à 2 fois plus élevé que le MPEG-4. La qualité DVD devrait pouvoir être atteinte en utilisant un bitrate de 2Mbps (250 Ko/sec) alors que la qualité VHS sera accessible dès le Mbps (125 Ko/sec).

De nombreuses entreprises misent sur H264. Plusieurs constructeurs de platines DVD (avec encodage sur disque dur intégré) et de téléphones mobiles espèrent pouvoir proposer très rapidement une compatibilité H264. Il faut dire que la licence pour exploiter H264 reste l'une des moins chères du marché (moins chère que MPEG2 ou MPEG4). La recommandation H264 est également étudiée pour être intégrée dans l'éventuel successeur du DVD, le DVD haute définition (HD-DVD). Dans ce domaine, H264 est en concurrence directe avec le Windows Média 9 de Microsoft.

Ce nouveau codec pose toutefois un problème, il est très gourmand en ressources mais le développement et la baisse des prix des composants électroniques de décompression devrait suffire à surmonter rapidement ce problème.

## 3.5.4 - Normes et standards

| | |
|---|---|
| RIT0082 | Il est OBLIGATOIRE d'utiliser la norme ISO 14496 (MPEG-4) pour les échanges de séquences vidéo Haute Définition. |
| RIT0083 | Il est RECOMMANDÉ d'utiliser la norme ISO 14496 (MPEG-4) pour la présentation de séquences vidéo Haute Définition. |
| RIT0084 | Il est RECOMMANDÉ d'utiliser la norme ISO 14496 (MPEG-4) pour la mise en oeuvre de services audiovisuels. |

| **Nom + Version** | **Spécification** | **Etat** | **Date** |
|---|---|---|---|
| MPEG-4 | ISO/IEC 14496<br>Codage des objets audiovisuels | Norme publiée | Oct 1998 |
| | ISO/IEC 14496 Version 2 | Norme publiée | 2000 |
| | ISO/IEC 14496-10 | | |
| | Recommandation H.264. Codage vidéo évolué pour les services audiovisuels génériques<br><br>http://www.itu.int/ITU-T/ | Approuvée | Mars 2005 |
| | http://www.mpeg.org/MPEG/starting-points.html#mpeg4<br><br>http://www.chiariglione.org/mpeg/ | | |

## 3.6 - Formats des données graphiques

### 3.6.1 - Description

| | |
|---|---|
| **Objectif** | Ces règles permettent de définir les formats d'échange de données métier entre les administrations et les usagers et de garantir ainsi l'interopérabilité. Les données graphiques sont des données administratives, sectorielles ou globales nécessitant l'utilisation de logiciels graphiques dédiés à la 2D, à la CAO, au dessin industriel, etc. |
| **Domaine d'interopérabilité** | • Intégration entre portails et téléservices<br>• Intégration entre portails et services administratifs<br>• Intégration entre téléservices<br>• Intégration entre téléservices et services techniques |
| **Responsable** | |

### 3.6.2 - Normes et standards

| | |
|---|---|
| RIT0017 | Il est RECOMMANDÉ d'utiliser la norme ISO 8632 (CGM) pour la mémorisation et l'échange de données graphiques à deux dimensions. |

CGM (Computer Graphics Metafile) est une norme de l'ISO pour la mémorisation et l'échange de données graphiques à deux dimensions (bitmap, texte ou vectoriel).

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| CGM<br>ISO 8632:1999<br>2ème édition | Infographie -- Métafichier de stockage et de transfert des informations de description d'images.<br>http://www.iso.org/iso/fr/ISOOnline.frontpage | Norme publiée | 1999 |

Il est possible de télécharger gratuitement cette norme à partir de l'adresse suivante :

http://isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf_Home/PubliclyAvailableStandards.htm

| | |
|---|---|
| RIT0018 | Il est RECOMMANDÉ d'utiliser la norme ISO 10303 (STEP) pour la représentation et l'échange d'informations sur les produits industriels dans le domaine de la CAO et de la production. |

STEP (Standard for the Exchange of Product Data) sont des normes pour la représentation et l'échange d'informations sur les produits industriels. Ces normes sont répandues dans le domaine de la Conception Assistée par Ordinateur (CAO) et de la production.

La norme internationale ISO 10303 fournit une représentation de l'information relative au produit ainsi que les mécanismes et définitions nécessaires pour permettre l'échange de données de produit. L'échange est réalisé entre différents systèmes et environnements informatiques associés à l'intégralité du cycle de vie du produit comprenant la conception, la fabrication, l'utilisation, la maintenance et la destruction finale du produit.

Rentrent dans le domaine d'application de l'ISO 10303 :

- la représentation de l'information relative au produit, comprenant les composants et les assemblages,
- l'échange des données de produit, comprenant le stockage, le transfert, l'accès et l'archivage.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| STEP<br>ISO 10303:1994 | Systèmes d'automatisation industrielle et intégration -- Représentation et échange de données de produits<br><br>http://www.iso.org/iso/fr/ISOOnline.frontpage | Norme publiée | 1994 |

Les principes de la norme ISO 10303 STEP sont disponibles à l'adresse suivante :

http://www.tc184-sc4.org/SC4%5FOpen/SC4%5FWork%5FProducts%5FDocuments/STEP%5F%2810303%29/

| | |
|---|---|
| RIT0019 | Il est RECOMMANDÉ d'utiliser le format DXF v19 pour les échanges de dessins techniques (par exemple des plans de construction). |
| RIT0020 | Il est DECONSEILLÉ d'utiliser le format DXF pour la présentation de dessins techniques puisqu'il nécessite l'utilisation d'un logiciel propriétaire. |

DXF signifie Drawing eXchange Format C'est un format propriétaire créé par la société Autodesk servant à échanger des fichiers DAO ou CAO entre systèmes CAO n'utilisant pas le même format de fichier natif.

DWG signifie DraWinG. C'est un format propriétaire utilisé par le logiciel de dessin industriel AutoCAD de la société Autodesk.

Le logiciel AutoCAD est incontournable dans le monde du dessin industriel.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| DXF<br>v.u19.1.01 | AutoCAD DXF Reference<br><br>http://www.autodesk.com | Proprié-taire | Fév 2004 |

## 3.7 - Formats des données de pré-impression

### 3.7.1 - Description

| | |
|---|---|
| **Objectif** | Ces règles visent à garantir l'interopérabilité entre les différents services techniques des administrations. Cela permet à une administration d'utiliser ou d'intégrer dans ses propres applications des services techniques mis à disposition par d'autres administrations, par exemple, accéder à un service d'impression centralisé. |
| **Domaine d'interopérabilité** | • Échange de données numériques de pré-impression<br>• Accès aux services d'impression centralisés |
| **Responsable** | |

### 3.7.2 - Normes et standards

| | |
|---|---|
| RIT0021 | Il est RECOMMANDÉ d'utiliser le format PDF/X (ISO 15930) pour l'échange de données numériques de pré-impression. |

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| ISO 15929:2002 | Échange de données numériques de pré-impression. Lignes directrices et principes d'élaboration des normes PDF/X. | Norme publiée | Mars 2002 |
| ISO 15930-1:2001 | Échange de données numériques de pré-impression - Emploi de PDF. http://www.iso.org/iso/fr/ISOOnline.frontpage | Norme publiée | Nov 2005 |

Le format PDF/X a été défini en 1998 par la société Adobe dans le cadre d'un partenariat avec des constructeurs, des associations d'utilisateurs et des organisations de normalisation comme l'ISO et l'ANSI. Les spécifications de ce format permettent d'assurer l'échange de documents PDF de manière fiabilisée dans le domaine de la pré-impression. Les fichiers PDF sont vérifiés avant leur envoi de façon à éviter les différences d'interprétation des RIP Postscript. La norme ISO 15930 se décline en trois versions :

PDF/X-1a (ISO 15930-1). Cette version est basée sur la version PDF 1.2. Elle est utilisée dans des environnements adaptés et présente la particularité de pouvoir incorporer les images haute résolution en fichiers attachés. Cette version est utilisée pour l'échange complet de données numériques.

PDF/X-2 (ISO 15930-2). Cette version n'oblige pas l'incorporation des polices et des images hautes résolutions. Elle permet donc l'échange de documents avec des ressources partielles, c'est à la réception que les ressources nécessaires seront complétées. Elle n'oblige pas l'incorporation des images haute résolution ni des polices et ne peut donc être utilisée dans un environnement ouvert. Cette version ne peut être utilisé pour une impression professionnelle.

PDF/X-3 (ISO 15930-3). Cette version est basée sur la version PDF 1.3. Elle autorise les gestions de la couleur plus étendue que le PDF/X-1a. Elle oblige l'encapsulation des polices utilisées et interdit les compressions du document, mais ne nécessite pas de connaître l'environnement dans lequel ont été préparés les fichiers PDF. Elle représente à ce jour le meilleur compromis entre liberté de création, fiabilité et possibilités de corrections.

# 4 - Interopérabilité des formats de document

## 4.1 - Documents non structurés et semi-structurés

### 4.1.1 - Description

| | |
|---|---|
| **Objectif** | Ces règles permettent de définir les formats d'échange de documents non structurés entre les administrations et les usagers et de garantir ainsi l'interopérabilité.<br>Un document non structuré est un document ayant une structuration libre, par exemple une page Web.<br>Un document semi structuré est un document ayant une partie structurée et une partie dont la structure est libre. De nombreux formats de document notamment ceux issus des logiciels bureautiques délivrent ce type de format (traitement de texte, tableur, présentation). |
| **Domaine d'interopérabilité** | Accès aux services en ligne |
| **Responsable** | |

### 4.1.2 - Normes et standards de présentation en ligne de documents

| | |
|---|---|
| RIT0022 | Il est RECOMMANDÉ d'utiliser le langage HTML 4.01 pour la présentation en ligne de documents non structurés. |
| RIT0023 | Il est INTERDIT d'utiliser le langage HTML 4.01 pour les échanges de documents non structurés puisque il s'agit d'un langage de présentation. |

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. HTML est une application du langage à balises SGML.

Le langage HTML est utilisé pour structurer et publier du contenu sur Internet. HTML 4.01 est le niveau actuel du standard HTML du W3C. Bien que la compatibilité ascendante soit assurée au niveau des navigateurs, on évitera l'utilisation d'un niveau inférieur de HTML, en particulier pour les nouveaux développements.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| HTML 4.01 | http://www.w3.org/TR/html4 | Recommandé | Déc 1999 |

### 4.1.3 - Evolution du standards HTML vers XHTML

XHTML (Extensible HyperText Markup Language) est un langage de balisage hypertexte extensible Il sert à l'écriture de pages Web et c'est le successeur de HTML.

En effet, le langage XHTML respecte la syntaxe définie par XML, plus récente et plus simple que la syntaxe définie par SGML respectée par HTML. On peut se reporter au chapitre « Formats des documents structurés » pour avoir la description de SGML et XML. La tendance à venir semble donc de migrer vers XHTML.

| **Nom + Version** | **Spécification** | **Etat** | **Date** |
|---|---|---|---|
| XHTML 1.1 | http://www.w3.org/MarkUp/ | Recommandé | Mai 2001 |
| XHTML 2.0 | http://www.w3.org/TR/2005/WD-xhtml2-20050527/ | Working Draft | Mai 2005 |

Les spécifications de XHTML 1.1, divisent le langage en modules de manière à ce que chaque module regroupe un type de fonctionnalités. Ce découpage est conçu pour permettre à du matériel informatique aux capacités techniques limitées de ne prendre en charge que des parties bien définies de XHTML.

Ceci donne la souplesse nécessaire pour permettre la consultation avec des appareils très divers : ordinateur de bureau, PC de poche, téléphone portable.

## 4.1.4 - Normes et standards d'échange de documents bureautiques

| | |
|---|---|
| RIT0024 | Il est RECOMMANDÉ d'utiliser des formats de document reposant sur l'utilisation d'XML et dont les spécifications sont publiques et libres de droit pour les échanges de documents bureautiques semi-structurés (traitement de texte, tableur, présentation). |
| RIT0025 | Il est RECOMMANDÉ d'utiliser le format Open Document pour les échanges de documents bureautiques semi-structurés (traitement de texte, tableur, présentation). |

| | |
|---|---|
| RIT0026 | Il est OBLIGATOIRE d'accepter tout document au format Open Document pour les échanges de documents bureautiques semi-structurés (traitement de texte, tableur, présentation). |
| RIT0027 | 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. |

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, auquel il reste similaire.

La version 1.0 a été approuvée par l'organisation OASIS en mai 2005. Par ailleurs, Open Document a été soumis à l'ISO le 30 Septembre 2005 pour ratification. Plus précisément, il a été soumis à la commission ISO/IEC JTC1 (ISO/International Electrotechnical Commission's Joint Technical Committee) pour devenir une norme de droit.

Il faut noter qu'OASIS est l'une des rares organisations autorisées par l'ISO à proposer ses standards suivant la procédure accélérée (*fast track)*, qui évite qu'un comité technique de l'ISO ait à dupliquer celui de l'OASIS.

| **Nom + Version** | **Spécification** | **Etat** | **Date** |
|---|---|---|---|
| Open Document v1.0 | OASIS Open Document Format for Office Applications (OpenDocument) TC http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=office | Standard approuvé OASIS. | mai 2005 |
| ISO/IEC DIS 26300 | Format de document ouvert pour applications de bureau (document ouvert) v1.0. | Projet de norme. Soumis à l'ISO | 31 oct 2005 |

http://www.iso.org/iso/fr/CatalogueDetailPage.CatalogueDetail?CSNUMBER=43485&scopelist=PROGRAMME

### 4.1.5 - Conservation des documents bureautiques

| | |
|---|---|
| RIT0029 | Il est OBLIGATOIRE d'utiliser le format PDF/A (norme ISO 19005) pour la conservation des documents non structurés et semi-structurés. |

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 elle 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, Acrobat Reader, sous réserve de l'acceptation du contrat de licence de l'Utilisateur Final. Ce contrat est disponible à l'adresse suivante :

http://www.adobe.fr/products/acrobat/acrreula.html

PDF/A-1 est une version restreinte basée sur PDF v1.4. Elle est normalisée par l'ISO.

PDF/A-1 optimise l'indépendance matérielle et logicielle ainsi que l'auto-documentation.

Les restrictions comportent :

- La non inclusion d'audio ou de vidéo,
- L'interdiction du lancement de JavaScript ou de fichiers exécutables,
- L'inclusion de toutes les polices de caractères et leur utilisation sans contrainte légale et d'affichage,
- La palette des couleurs utilisée doit être spécifiée de manière indépendante,
- L'interdiction du chiffrement,
- L'utilisation de méta-données standard est obligatoire.

| **Nom + Version** | **Spécification** | **Etat** | **Date** |
|---|---|---|---|
| PDF/A-1<br><br>ISO 19005-1:2005 | Format de fichier des documents électroniques pour une conservation à long terme. Partie 1 : Utilisation du PDF 1.4 (PDF/A-1). | Norme publiée | Sept. 2005 |

http://www.iso.org/iso/fr/CatalogueDetailPage.CatalogueDetail?CSNUMBER=38920&ICS1=37&ICS2=100&ICS3=99

### 4.1.6 - Principes de mise en oeuvre

*Il n'existe pas encore d'élément référencé.*

### 4.1.7 - Composants

*Il n'existe pas encore d'élément référencé.*

### 4.1.8 - Exemples d'initiatives sectorielles

La gendarmerie nationale a adopté une suite bureautique qui intègre le format OpenDocument et privilégie ce format d'échange tant en interne qu'avec les autres administrations. Cette expérimentation à grande échelle permet d'estimer l'impact sur le SI de la gendarmerie d'une part et sur les SI des autorités administratives partenaires de la gendarmerie.

Cette initiative permet également d'identifier les solutions mises en œuvre pour obtenir une interopérabilité avec les SI ne disposant pas d'outils permettant nativement de présenter, traiter et échanger sous ce format.

## 4.2 - Documents structurés

### 4.2.1 - Description

| | |
|---|---|
| **Objectif** | Ces règles de définir les formats d'échange de documents structurés entre les administrations et les usagers ainsi qu'entre administrations afin de garantir ainsi l'interopérabilité.<br>Un document structuré est un document supportant un format, par exemple des extraits de bases de données. |
| **Domaine d'interopérabilité** | • Accès aux services en ligne<br>• Intégration entre portails et téléservices<br>• Intégration entre portails et services administratifs<br>• Intégration entre téléservices<br>• Intégration entre services techniques<br>• Intégration entre téléservices et services techniques |
| **Responsable** | |

### 4.2.2 - Normes et standards

Pour la description de la norme sur l'encodage des caractères, se reporter au chapitre précédent.

| | |
|---|---|
| RIT0030 | Il est RECOMMANDÉ d'utiliser le langage XML 1.1 pour formater des documents structurés. |
| RIT0031 | Il est OBLIGATOIRE d'utiliser le langage XML 1.1 pour échanger des données structurées. |
| RIT0032 | Il est OBLIGATOIRE d'utiliser le langage XML 1.1 comme format d'échange si les documents structurés source ne sont pas au format XML. |

XML (Extensible Mark-Up Language) est basé sur le langage SGML (ISO 8879). Il a été conçu et promu par l'association W3C (World Wide Web Consortium) qui est un acteur référent dans le domaine Internet.

Par exemple, les différents composants de la suite bureautique OpenOffice.org sauvegardent leurs données au format XML.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| XML 1.1 | http://www.w3.org/TR/2004/REC-xml11-20040204/ | Recommandation | Fév 2004 |

| | |
|---|---|
| RIT0033 | Il est RECOMMANDÉ d'utiliser XML Schema pour la modélisation ou l'échange du format de description des documents structurés. |

XML Schema est un langage de description de format de document XML. Il permet de décrire la structure d'un document XML. Un schéma XML est lui-même un fichier XML. La connaissance de la structure d'un document XML permet notamment de vérifier la validité de ce document. Un fichier de description de structure (*XML Schema Description* en anglais, ou fichier *XSD*) est donc lui-même un document XML.

XML Schema s'utilise pour spécifier des formats de documents ou pour valider que des documents sont conformes à la structure spécifiée.

| **Nom + Version** | **Spécification** | **Etat** | **Date** |
|---|---|---|---|
| XML Schema | http://www.w3.org/TR/xmlschema-0/<br><br>http://www.w3.org/TR/xmlschema-1/<br><br>http://www.w3.org/TR/xmlschema-2/ | Recommandé | 28 oct 2004 |

| | |
|---|---|
| RIT0035 | Il est RECOMMANDÉ d'utiliser le langage XForms pour la description des formulaires en XML. |

XForms est un format basé sur XML qui permet de décrire des formulaires structurés. XForms gère séparément la présentation et le contenu et 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.

| **Nom + Version** | **Spécification** | **Etat** | **Date** |
|---|---|---|---|
| XForms v1.0 | http://www.w3.org/TR/xforms/ | Recommandation | Oct 2003 |
| XForms v1.1 | http://www.w3.org/TR/2005/WD-xforms11-20051209/ | Working Draft | Déc 2005 |

| | |
|---|---|
| RIT0036 | Il est DÉCONSEILLÉ d'utiliser SGML ISO 8879 pour la description des documents structurés. |

SGML (Structured General Mark-Up Language) est un langage de balisage. Il est utilisé pour la description de documents. Les langages HTML et XML ont été créés à partir de SGML.

L'utilisation de XML, de préférence à SGML, est recommandée.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| SGML<br>ISO 8879:1986 | Systèmes bureautiques -- Langage normalisé de balisage généralisé.<br><br>http://www.iso.org/iso/fr/ISOOnline.frontpage | Norme publiée | Août 2001 |

| | |
|---|---|
| RIT0037 | Il est DÉCONSEILLÉ d'utiliser un DTD (Document Type Declaration) pour la modélisation ou l'échange du format de description des documents structurés. |

Un DTD (Définition de Type de Document), est un document permettant de décrire un modèle de document SGML ou XML Toutefois, il ne décrit que la structure du document. Bien qu'inclus dans la version 1.0 de la spécification d'XML, le langage DTD est souvent délaissé au profit du langage « XML Schema » (décrit plus haut) pour les raisons suivantes :

- Pas de support des dernières caractéristiques d'XML (par exemple, les « namespaces »).
- Syntaxe non-XML hérité du langage SGML.

| | |
|---|---|
| RIT0034 | Il est RECOMMANDÉ d'utiliser le format XML pour réaliser des exports de bases de données. |

## 4.3 - Les langages XSLT et XPath

### 4.3.1 - Description

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.

XPath est une syntaxe pour désigner une portion d'un document XML. Initialement créé pour fournir une syntaxe et une sémantique aux fonctions communes à XPointer et XSL, XPath a rapidement été adopté par les développeurs comme un petit langage d'interrogation.

### 4.3.2 - Normes et standards

Standard à suivre pour une prise en compte ultérieure (lorsque le standard sera industriellement reconnu).

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| Outils de traitement et de présentation des données | XSL (Extensible Stylesheet Language) XSLT 2.0<br><br>http://www.w3.org/TR/xslt20 | « Draft » W3C | Nov 2002 |
| | XPath 2.0<br><br>http://www.w3.org/TR/xpath20 | « Draft » W3C | Nov 2002 |

### 4.3.3 - Tendances d'évolution

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 du langage 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.

# 5 - Recommandations sur les IHM

## 5.1 - Accessibilité et ergonomie des IHM Web

### 5.1.1 - Description

| | |
|---|---|
| **Objectif** | Ces règles visent à garantir l'accessibilité et l'ergonomie des services en ligne de l'administration électronique, à tous les usagers et agents publics. |
| **Domaine d'interopérabilité** | Accès aux services en ligne |
| **Responsable** | |

### 5.1.2 - Normes et standards

| | |
|---|---|
| RIT0039 | Il est RECOMMANDÉ de respecter les recommandations de l'ISO, du CEN/CENELEC et du W3C, concernant l'accessibilité et l'ergonomie des services en ligne de l'administration électronique. |

Ces recommandations du W3C décrivent les moyens de rendre accessibles les sites web aux usagers handicapés.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| ISO/TS 16071:2003 | Ergonomie de l'interaction homme/système -- Guidage relatif à l'accessibilité aux interfaces homme/ordinateur.<br><br>http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=30858&ICS1=13&ICS2=180&ICS3= | Norme publiée | Mai 2003 |
| ISO/IEC Guide 71:2001 | Principes directeurs pour les normalisateurs afin de répondre aux besoins des personnes âgées et de celles ayant des incapacités.<br><br>http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33987&ICS1=1&ICS2=120&ICS3 | Norme publiée | Juill 2005 |
| CEN/CENELEC Guide 6 | Guidelines for standards developers for older persons and persons with disabilities.<br><br>http://www.cenorm.be/cenorm/businessdomains/businessdomains/isss/activity/cclcgd006.pdf | Recommandé | Jan. 2002 |
| Authoring Tool Accessibility Guidelines 1.0 | www.w3.org/TR/ATAG10/ | Adopté | Fév 2000 |
| User Agent Accessibility Guidelines 1.0 | www.w3.org/TR/UAAG10/ | Adopté | Déc. 2002 |
| Web Content Accessibility Guidelines 1.0 | www.w3.org/TR/1999/WAI-WEBCONTENT-19990505 | Recommandé | Mai 1999 |

## 5.1.3 - Principes de mise en œuvre Accessibilité

| | |
|---|---|
| RIT0040 | Il est OBLIGATOIRE de se conformer au « Référentiel accessibilité des services de communication publique en ligne de l'administration française » pour la mise en œuvre de sites et services Intranet et Internet. |

Ce Référentiel a pour objet de définir un cadre technique, méthodologique et organisationnel en matière d'accessibilité des services de communication publics en ligne de l'administration française.

Il présente l'ensemble des critères nécessaires pour que les services soient non seulement accessibles à tous les usagers mais présentent en plus un confort d'utilisation et de navigation optimisé, quel que soit le canal utilisé (Web, téléphone, TV numérique, …).

A ce titre, il est composé de parties distinctes traitant de chaque canal, le canal Web étant le plus développé à ce jour.

- La première partie présente les critères d'accessibilité tels que définis dans les recommandations internationales WCAG version 1.0 du W3C/WAI (Orientations pour l'accessibilité du contenu du web) (Web Content Accessibility Guidelines). Ces critères sont issus des travaux AccessiWeb (http://www.accessiweb.org), méthode d'application de ces recommandations internationales ;
- La seconde partie présente les critères de facilité d'utilisation. Ces critères sont notamment issus des travaux de Jakob Nielsen et de Marie Tahir, experts internationaux reconnus dans ce domaine (pour plus de détail sur ce sujet se reporter au site http://www.useit.com/).

| **Nom + Version** | **Spécification** | **Etat** | **Date** |
|---|---|---|---|
| Référentiel accessibilité des services de communication publique en ligne de l'administration française. V1.0 | http://www.adae.gouv.fr/spip/rubrique.php3?id_rubrique=46 | Publié | 2004 |
| V2.0 | Spécifications en cours de rédaction | En cours | juin 2006 |

## 5.1.4 - Principes de mise en œuvre Ergonomie

| | |
|---|---|
| RIT0072 | Il est OBLIGATOIRE, pour une administration qui met à disposition des usagers, une téléprocédure publique sur un site Web du domaine « gouv.fr », de se conformer à la « Charte Graphique et Ergonomique des Téléprocédures publiques ». |
| RIT0073 | Il est RECOMMANDÉ, pour une administration qui met à disposition des usagers, une téléprocédure publique sur un site Web hors du domaine « gouv.fr », de se conformer à la « Charte Graphique et Ergonomique des Téléprocédures publiques ». |
| RIT0074 | Il est RECOMMANDÉ, pour les autres sites des administrations, de se conformer à la « Charte Graphique et Ergonomique des Téléprocédures publiques ». |

Les téléprocédures publiques sont des déclarations et demandes administratives mises à disposition des usagers par formulaire guidé en ligne. L'objectif de cette charte est de fournir des règles ergonomiques et graphiques. Elle a été rédigée par un groupe interministériel animé par la DGME.

Plus particulièrement, les objectifs de la Charte sont de :

- Fournir un niveau de confort minimum aux utilisateurs quelque soit l'émetteur de la téléprocédure,
- Donner une identité visuelle au site, tant en termes de graphisme que de navigation,
- Faciliter et accélérer le travail du concepteur en proposant des principes de composition, de navigation et de repérage.

Cette charte définit trois niveaux de labellisation d'un site : OR, ARGENT et BRONZE.

| | |
|---|---|
| RIT0097 | Il est OBLIGATOIRE, pour une administration mettant à disposition une téléprocédure publique, de se conformer à la labellisation indiqué dans le scénario de migration décrit dans la « Charte Graphique et Ergonomique des Téléprocédures publiques ». |

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| Charte V1.0 | Charte Graphique et Ergonomique des Téléprocédures publiques | En appel public à commentaires | Avril 2006 |

### 5.1.5 - Composants

*Il n'existe pas encore d'élément référencé.*

### 5.1.6 - Exemples d'initiatives sectorielles

*Il n'existe pas encore d'élément référencé.*

### 5.1.7 - Autres exemples

Concernant le serveur Web « Europa Le portail de l'Union européenne », la politique d'accessibilité du contenu est décrite à l'adresse suivante :

http://europa.eu.int/geninfo/accessibility_policy_fr.htm

## 5.2 - Technologies pour construire les IHM Web

### 5.2.1 - Description

| | |
|---|---|
| **Objectif** | Les technologies disponibles pour construire les interfaces d'applications Web sont nombreuses et il convient donc de s'accorder sur certains standards et principes de mise en œuvre de manière à :<br>• Garantir l'accessibilité des services en ligne de l'administration Electronique au plus grand nombre d'utilisateurs,<br>• Garantir l'interopérabilité des services en ligne entre administrations. |
| **Domaine d'interopérabilité** | Accès aux services en ligne |
| **Responsable** | |

### 5.2.2 - Normes et standards

| | |
|---|---|
| RIT0041 | Il est RECOMMANDÉ d'utiliser le langage HTML 4.01 pour construire les interfaces d'applications Web des services en ligne de l'administration. |

Le langage HTML est utilisé pour structurer et publier du contenu sur Internet. Il est en particulier utilisé pour construire les interfaces d'applications Web. HTML 4.01 est le niveau actuel du standard HTML du W3C. Bien que la compatibilité ascendante soit assurée au niveau des navigateurs, on évitera l'utilisation d'un niveau inférieur de HTML, en particulier pour les nouveaux développements.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| HTML 4.01 | http://www.w3.org/TR/html4/<br><br>avec une traduction en français http://www.la-grange.net/w3c/html4.01/cover.html | Recommandé | 24 déc 1999 |

| | |
|---|---|
| RIT0042 | Il est RECOMMANDÉ d'utiliser CSS niveau 2 pour ajuster la présentation de documents structurés. |

Les feuilles de styles (Cascading Style Sheet ou CSS) permettent de spécifier l'habillage et la mise en page des documents structurées (HTML, XML, etc.) mais aussi des IHM des applications Web de l'administration Electronique. Le niveau 2 de CSS étend le niveau 1 et permet notamment d'adapter la présentation à différents modes d'accès de l'utilisateur (navigateurs graphiques, imprimantes, terminaux braille, etc.).

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| CSS niveau 2 | Cascading Style Sheet level 2<br>http://www.w3.org/TR/CSS2/ | Recommandé | 12 mai 1998 |

| | |
|---|---|
| RIT0043 | Il est DÉCONSEILLÉ d'utiliser des langages de script (JavaScript, ECMAScript, Jscript, etc) ou des applets Java pour créer des IHM Web. |

L'interopérabilité entre les différents navigateurs (Internet Explorer, FireFox, etc.) n'est pas assurée pour l'exécution de scripts (JavaScript, ECMAScript, Jscript) ou l'exécution d'applets Java au niveau du poste client.

Ainsi, leur utilisation au niveau d'un téléservice est possible mais DOIT être réservée à des fonctionnalités « optionnelles » ou « de confort » (par exemple, auto-completion, prévalidation de champs avant envoi au serveur, etc.). Dans le cadre de la dématérialisation de formulaires, cette fonction de prévalidation de champs peut être utilisée avec beaucoup d'intérêt. La fonctionnalité du téléservice DOIT rester accessible à travers un navigateur sans utilisation de scripts ou d'applets Java.

**Attention : il existe une exception notable concernant la signature électronique en ligne qui nécessite l'utilisation d'applets Java.**

**D'une manière générale, si un service en ligne de l'administration nécessite l'utilisation de fonctions particulières ou la mise en œuvre d'un client riche, ceci sera clairement indiqué.**

**Dans ce cas, il sera préférable de se rapprocher de la norme ISO 16262 (ECMA-262) qui spécifie le langage ECMAScript. L'utilisation de la méthode de développement d'applications Web, AJAX (Asynchronous JavaScript And XML) est également une solution possible.**

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| ECMA-262 | ECMAScript Language Specification http://www.ecma-international.org/publications/standards/Ecma-262.htm | | Déc 1999 |
| ISO/IEC 16262:2002 | ECMAscript spécifications du langage. | Norme publiée | Juin 2002 |

http://www.iso.org/iso/fr/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33835&ICS1=35&ICS2=60&ICS3=

| | |
|---|---|
| RIT0044 | Il est INTERDIT d'utiliser des composants logiciels type ActiveX ou toute autre extension de navigateur (Flash hors animation, VML, etc.) au niveau des IHM Web. |

Pour des raisons de facilité d'utilisation du téléservice et d'incompatibilité technique entre navigateurs, les IHM Web des téléservices ne doivent pas nécessiter l'installation et/ou l'exécution d'ActiveX (ou d'autres extensions de navigateur) sur le poste client.

### 5.2.3 - Exemples d'initiatives sectorielles

- Ministère des Affaires Etrangères : Normes de réalisation Internet d'un client léger - Version 2.3
- Ministère des Affaires Etrangères : Normes de réalisation Internet d'un client riche - Version 2.0

## 5.3 - Compatibilité des IHM avec les Navigateurs

En janvier 2006, au niveau mondial, Microsoft-Internet-Explorer et Mozilla-Firefox représentent environ 97 % des navigateurs installés.

### 5.3.1 - Normes et standards

| | |
|---|---|
| RIT0045 | Il est OBLIGATOIRE que les applications destinées aux usagers soient compatibles avec les versions de navigateurs mentionnés dans le RGI. |
| RIT0092 | Il est RECOMMANDÉ que les applications destinées aux agents soient compatibles avec les versions de navigateurs mentionnés dans le RGI. |

### 5.3.2 - Tableau des navigateurs

| **Nom + Version** | **Spécification** | **Etat** | **Date** |
|---|---|---|---|
| Internet-Explorer v6 et ultérieures | Versions Windows 2000 et XP | diffusée | |
| Mozilla-Firefox V1.0.7 et ultérieures | Versions Windows 2000 et XP | diffusée | |
| Mozilla-Firefox V1.0.7 et ultérieures | Versions Mac OS X 10.4 et ultérieures | diffusée | |
| Mozilla-Firefox V1.0.7 et ultérieures | Versions Linux (x86) noyau 2.4 et ultérieures | diffusée | |

### 5.3.3 - Principes de mise en oeuvre

| | |
|---|---|
| RIT0095 | Il est RECOMMANDÉ d'optimiser l'affichage des pages Web sur les navigateurs, en paramétrant les écrans d'ordinateurs avec une résolution de 1024 par 768 pixels. |

## 5.4 - Intégration de services Web par les IHM

### 5.4.1 - Description

| | |
|---|---|
| **Objectif** | Ces règles visent à garantir l'interopérabilité entre les portails, téléservices et services administratifs en ligne afin, par exemple, de pouvoir intégrer dans le portail d'une administration des services fournis par une autre administration. |
| **Domaine d'interopérabilité** | • Intégration entre portails,<br>• Intégration entre portails et téléservices,<br>• Intégration entre portails et services administratifs,<br>• Intégration entre téléservices. |
| **Responsable** | |

Les portlets et les servlets sont des composants web conçus pour être agrégés dans une page composite. Portlet est une interface permettant d'appeler les applications ou d'intégrer du contenu métier. Ceci permet de rendre les applications consultables au niveau de la page d'accueil d'un portail. Chaque utilisateur se voit attribué des droits particuliers ce qui permet de personnaliser la consultation.

Deux principaux protocoles standardisent l'utilisation des portlets : WSRP et JSR 168 (Portlet specification).

### 5.4.2 - Normes et standards Intégration de composants locaux

| | |
|---|---|
| RIT0046 | Il est RECOMMANDÉ de s'appuyer sur l'interface de programmation « Java Portlet Specification » pour intégrer des composants locaux dans un portail Web en environnement Java. |

La JSR 168 (Java Specification Request) de Sun définit un format de composants, les « Portlets », pouvant être intégrées au niveau d'un portail Web. Ces spécifications ne s'appliquent que dans le cas d'applications JAVA.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| JSR-168 Portlets API V1.0 | http://www.jcp.org/en/jsr/detail?id=168 | Finalisé | 27 oct 2003 |

## 5.4.3 - Normes et standards Intégration de composants distants

| | |
|---|---|
| RIT0047 | Il est RECOMMANDÉ d'utiliser le service WSRP pour intégrer des composants distants dans un portail Web. |

WSRP (« Web Services for Remote Portlets ») est une recommandation proposée par le consortium OASIS. Elle définit un moyen d'accéder à des « portlets » distantes à l'aide de Web Services. Son objectif est d'augmenter le niveau d'interopérabilité des services web produisant du contenu directement utilisable par un Internaute.

Une partie de la spécification de WSRP est commune avec la spécification WSIA de l'OASIS, qui vise quant à elle, l'interopérabilité des services web interactifs.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| WSRP 1.0 | http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsrp | Standard | Août 2003 |

## 5.4.4 - Normes et standards Intégration et compatibilité

| | |
|---|---|
| RIT0048 | Il est INTERDIT d'utiliser des tags IFRAME pour intégrer des services distants. |

Le tag HTML « IFRAME » est une forme particulière de « FRAME » qui se charge à l'intérieur d'une page. Cela permet plusieurs types d'utilisations. Par exemple, il est possible d'afficher plusieurs pages d'informations sur un seul écran ou encore de donner un aperçu sur un site extérieur sans quitter le site initial.

Toutefois, la compatibilité n'est pas assurée d'un navigateur à l'autre, d'où l'interdiction.

## 5.5 - Syndication de contenu

### 5.5.1 - Normes et standards Le format RSS

| | |
|---|---|
| RIT0049 | Il est RECOMMANDÉ d'utiliser le format RSS pour réaliser de la syndication de contenu Web de type « fil d'information ». |

RSS (Really Simple Syndication) et HTML présentent une similitude de perspective. Ces deux langages servent à formater des données. HTML permet de styliser des contenus ; RSS permet d'en agréger, ce que l'on retrouve derrière le terme importé de l'anglais de *syndication* (rassemblement). RSS décrit un format de document XML permettant de réaliser de l'agrégation de contenu. C'est un langage de formatage des données simple et en très forte expansion sur Internet.

RSS peut être utilisé de deux manières :

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

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| RSS 2.0.1 | http://blogs.law.harvard.edu/tech/rss | | 2002 |

### 5.5.2 - Normes et standards Le format ATOM Syndication

| | |
|---|---|
| RIT0050 | Il est DÉCONSEILLÉ d'utiliser le format ATOM Syndication pour réaliser de la syndication de contenu Web. |

Atom est un format de document basé sur XML conçu pour la syndication de contenu périodique tel que les weblogs ou les sites d'actualités. Il permet l'affichage des sources surveillées aussi bien sur un site Web que directement dans un agrégateur. Il est semblable aux diverses versions de RSS, mais vise à être plus flexible. Il est normalisé par l'IETF (le RFC est approuvé mais pas encore publié) contrairement aux divers RSS, pilotés par des entreprises privées. Les fils Atom peuvent être distribués, par exemple par le protocole HTTP. Le schéma XML utilisé est spécifié grâce au langage RelaxNG.

Le format expérimental Atom 0.3 semble, à l'heure actuelle, le plus répandu sur l'Internet. Le format officiel, le 1.0, est décrit dans le RFC 4287.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| Atom 1.0 | http://www.atomenabled.org/ | En phase de finalisation | |
| | RFC 4287 The Atom Syndication Format http://www.ietf.org/rfc/rfc4287.txt | Proposé Standard | Déc 2005 |

### 5.5.3 - Comparatif des formats

Des travaux de rapprochement sont en cours entre Atom Syndication Format (soumis à IETF) et RSS. Un comparatif des deux formats est disponible à l'adresse suivante :

http://www.intertwingly.net/wiki/pie/Rss20AndAtom10Compared

### 5.5.4 - Exemple d'utilisation

Le format RSS est notamment utilisé pour la diffusion d'actualités sur Internet. Ce système est très utilisé pour diffuser les nouvelles des sites d'information (actualité, sciences, informatique, etc.) ou des blogs, ce qui permet de consulter ces dernières sans visiter le site, ou bien de les formater à sa guise, etc.

Il existe sept formats différents de RSS, ce qui rend indispensable l'établissement d'une norme. Il est à noter que Syndicate, en anglais, est en rapport avec le journalisme et la vente d'un article à plusieurs journaux. Mais en fait le standard permet de diffuser toutes sortes d'information, d'alertes, de mise à jour de listes ou d'événements.

Really Simple Syndication se rapproche donc d'une diffusion journalistique simplifiée.

# 6 - Interopérabilité des messageries électroniques

## 6.1 - Protocole de Messagerie électronique

### 6.1.1 - Description

| | |
|---|---|
| **Objectif** | Ces règles définissent l'interopérabilité des échanges de messages électroniques entre les agents publics et les usagers. |
| **Domaine d'interopérabilité** | • Accès aux services en ligne,<br>• Intégration entre services techniques. |
| **Responsable** | Michel Zurbach |

### 6.1.2 - Normes et standards

| | |
|---|---|
| RIT0051 | Il est OBLIGATOIRE d'utiliser le protocole SMTP (« Simple Mail Transfer Protocol ») pour l'échange de messages électroniques. |

SMTP est le protocole utilisé pour le transport des messages électroniques (appelé aussi courriers électroniques ou courriels) sur Internet. Son usage est obligatoire pour l'envoi de courriels aux usagers et aux agents publics. ESTMP décrit des extensions au 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 au protocole 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-administrations.

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.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| SMTP | RFC 2821 Mise à jour et clarification sur SMTP | Proposé Standard | Avril 2001 |
| | RFC 2822 Internet Message Format | Proposé Standard | Avril 2001 |
| | RFC 2156 Mapping entre X400 et MIME | Proposé Standard | Janv 1998 |

## 6.2 - La représentation des messages et pièces jointes

### 6.2.1 - Normes et standards

| | |
|---|---|
| RIT0052 | Il est OBLIGATOIRE d'utiliser le protocole MIME (« Multipurpose Internet Mail Extensions ») pour la représentation des messages électroniques et des pièces jointes. |

MIME est le protocole utilisé pour la représentation des messages électroniques sur Internet. Son usage est obligatoire pour l'envoi de courriels aux usagers et aux agents publics.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| MIME | RFC 2045 Format of Internet Message Bodies | Draft Standard | nov 1996 |
| | RFC 2046 Media Types | Draft Standard | nov 1996 |
| | RFC 2047 Message Header Extensions for Non-ASCII Text | Draft Standard | nov 1996 |
| | RFC 2048 Registration Procedures | Recommandé | nov 1996 |
| | RFC 2049 Conformance Criteria and Examples | Draft Standard | nov 1996 |

## 6.3 - La sécurisation de la Messagerie électronique

### 6.3.1 - Normes et standards

| | |
|---|---|
| RIT0053 | Il est OBLIGATOIRE d'utiliser l'extension S/MIME pour sécuriser les envois de messages électroniques. |

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

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| S/MIME | RFC 2632 Support des certificats dans S/MIME v3 | Proposé Standard | Juin 1999 |
| | RFC 2633 Spécification des messages S/MIME v3 | Proposé Standard | Juin 1999 |
| | RFC 2634<br>Services de sécurité étendus pour S/MIME | Proposé Standard | Juin 1999 |
| | RFC 3369 Définit la syntaxe pour signer, condenser, authentifier ou chiffrer le contenu d'un message | Proposé Standard | Août 2002 |
| | RFC 3370 Définit les conventions d'utilisation des algorithmes de cryptographie | Proposé Standard | Août 2002 |

## 6.4 - L'accès aux B.A.L. de la Messagerie électronique

### 6.4.1 - Normes et standards

| | |
|---|---|
| RIT0054 | Il est OBLIGATOIRE d'utiliser le protocole POP3 (« Post Office Protocol ») ou le protocole IMAP4 (« Internet Message Access Protocol ») pour relever les messages électroniques déposés dans une boîte aux lettres. |

POP3 et IMAP4 sont des protocoles utilisés pour l'accès aux boîtes aux lettres électroniques (BAL).

IMAP (Interactive Mail Access Protocol) est moins utilisé que POP mais qui offre plus de possibilités. Il gère plusieurs accès simultanés, ainsi que plusieurs boîtes aux lettres sur le serveur, et il permet les recherches de courrier selon des critères. Il est plus riche mais plus complexe. IMAP devrait progressivement remplacer POP

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| POP V3 | RFC 1939 Spécifications du protocole | Standard | Mai 1996 |
| | RFC 1959<br>Observations sur les implémentations | Informationnel | Juin 1996 |
| | RFC 2449 Mécanismes d'extension | Proposé Standard | Nov 1998 |
| POP3 et IMAP4 | RFC 2595<br>Utilisation de TLS avec POP3 et IMAP4 | Proposé Standard | Juin 1999 |
| IMAP4 | RFC 3501 IMAP4 version 4 révision 1 | Proposé Standard | Mars 2003 |

## 6.5 - Les extensions à la Messagerie électronique

### 6.5.1 - Normes et standards

| | |
|---|---|
| RIT0085 | Il est RECOMMANDÉ d'utiliser l'extension ESMTP pour implémenter les fonctionnalités supplémentaires au protocole SMTP. |

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| ESMTP | RFC 1652 8bit MIME transport | Draft Standard | Juil 1994 |
| | RFC 1870 Message Size Declaration | Standard | Nov 1995 |
| | RFC 2920 Command Pipelining | Standard | Sept 2000 |
| | RFC 3461 Delivery Status Notifications | Draft Standard | Jan 2003 |
| | RFC 3462 The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages | Draft Standard | Jan 2003 |
| | RFC 3463<br>Enhanced Mail System Status Codes | Draft Standard | Jan 2003 |
| | RFC 3464 An Extensible Message Format for Delivery Status Notifications | Draft Standard | Jan 2003 |
| | RFC 3798 Message Disposition Notification | Draft Standard | Mai 2004 |
| | RFC 3885 Message Tracking | Proposé standard | Sept 2004 |
| | RFC 3886 An Extensible Message Format for Message Tracking Responses | Proposé standard | Sept 2004 |

Ils existent des extensions au protocole SMTP. Certaines sont obsolètes et remplacées par des extensions plus récentes à savoir les RFC 1891 à 1894 sont rendues obsolètes par les RFC 3461 à 3464.

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.

Remarques : 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).

## 6.6 - L'utilisation des services de messagerie par les applications EDI

### 6.6.1 - Normes et standards

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 les services de messagerie afin d'échanger de façon sécurisée des données structurées.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| MIME | RFC 3335<br>Echange de messages EDI avec MIME | Proposé Standard | Sept 2002 |

## 6.7 - Mise en œuvre de la Messagerie électronique

| | |
|---|---|
| RIT0056 | Il est OBLIGATOIRE pour les administrations de se conformer aux règles de dénomination des adresses électroniques définies dans la « Charte de Nommage Internet » v1.2 établie par l'administration. |

Le document « Charte de Nommage Internet » expose les règles à respecter pour la création des adresses Internet au sein de l'administration française. Ces règles doivent être respectées pour le choix des noms de domaine, des adresses personnelles des agents et des adresses des entités fonctionnelles. Ces règles permettent d'une part de normaliser les noms de domaine et les adresses électroniques dans l'administration et d'autre part d'organiser logiquement le sous-domaine « .gouv.fr ».

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| Charte de Nommage Internet v 1.2 | Voir ci-après. | Obligatoire | 23 oct 2001 |

http://www.adae.gouv.fr/upload/documents/Annexe_3c_regles_nommage.pdf

## 6.8 - Les passerelles de communications avec les terminaux GSM

Ce thème vise à définir les possibilités l'interopérabilité entre les différents services des administrations et les usagers via des terminaux conformes au protocole GSM.

### 6.8.1 - Normes et standards applicables

Ce paragraphe est en cours de rédaction.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| GSM | | | |
| SMS | | | |
| MMS | | | |

### 6.8.2 - Exemples d'initiatives sectorielles

Il existe un service d'envoi par SMS de notification d'avancement d'une télécandidature ANPE.

Il existe également un service d'envoi par SMS de notification d'absence des élèves au collège ou au lycée utilisé par l'Education nationale. Les SMS sont envoyés aux parents.

## 6.9 - Services de messagerie instantanée

L'objet du sous-chapitre est de faire apparaître ce service, de manière à faire ressortir l'expression d'un éventuel besoin conduisant à l'introduction du protocole au référentiel mais dans une version ultérieure.

### 6.9.1 - Principes

La messagerie instantanée, aussi abrégée *IM* du sigle anglophone d'*Instant Messaging*, permet de communiquer par ordinateur avec un interlocuteur distant connecté au même réseau informatique, notamment Internet. Contrairement au courrier électronique classique, la communication est conçue pour être instantanée. La messagerie instantanée est une idée assez ancienne : sous UNIX elle existe depuis bien longtemps, grâce à la commande *talk*, puis sous Windows, il y a eu l'équivalent avec *WinPopUp*. Le protocole IRC fournit lui aussi depuis 1988, des fonctionnalités de messagerie instantanée avancée.

La relation entre les deux interlocuteurs est de type « peer to peer » que l'on peut traduire par « pair-à-pair ». C'est une architecture où chaque ordinateur est à la fois client et serveur (très différent donc du client/serveur classique). La messagerie instantanée grand public a été révélée, par l'arrivée du produit ICQ en 1996. En évoluant, la messagerie instantanée intègre les fonctionnalités de voix et de vidéo grâce à une webcam.

La plupart de ces protocoles ont été introduits par les fournisseurs de contenu arrivés sur Internet un peu avant 2000. L'avantage pour eux était, en forçant l'utilisation d'un protocole fermé et de logiciels client précis, de pouvoir envoyer de la publicité aux abonnés et de se constituer des bases clients facilement.

L'arrivée de Jabber, qui propose un protocole ouvert, standard et normalisé, ce qui garantit son indépendance, plusieurs serveurs modulaires et plusieurs clients, bouscule les acteurs qui s'étaient taillé la part du lion sur ce marché en plein essor.

### 6.9.2 - Protocoles

IRC, acronyme de Internet Relay Chat (en français, discussion relayée par Internet), est un protocole de communication sur Internet. Il sert à la communication instantanée, prédécesseur de la messagerie instantanée. Conçu en 1988, il a été décrit initialement dans la RFC 1459, puis révisé dans les RFC 2810 à 2813.

Le protocole de communication décrit un réseau informatique formé de plusieurs serveurs connectés dans lequel les clients communiquent généralement par le biais du serveur (qui relayera éventuellement le message au reste du réseau). Il est également possible de connecter deux clients directement pour une conversation privée ou un transfert de fichier, on parle alors de DCC (*Direct Client-to-Client*). Ce protocole étant public, il existe des logiciels clients pour de nombreux systèmes d'exploitations, de même que les serveurs IRC, aussi désignés par le terme IRCD qui signifie Internet Relay Chat Daemon.

Il existe différents réseaux, qui sont le plus souvent libres d'utilisation et gratuits. Avec l'arrivée des gros fournisseurs de contenu un peu avant l'an 2000, le succès d'IRC a été quelque peu diminué. Ces réseaux restent néanmoins très utilisés par ceux qui veulent discuter sans passer par un programme client propriétaire ou n'offrant pas l'interactivité sous forme de *canaux*, permettant ainsi de rejoindre des milliers d'usagers.

### 6.9.3 - Normes et standards

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| IRC | RFC 1459<br>Protocole de discussion relayée par Internet | Expérimental | Mai 1993 |
| | RFC 2810 à 2813<br>Architecture et protocole | Expérimental | Avril 2000 |

# 7 - Interopérabilité des services d'annuaire

## 7.1 - Le Service d'annuaire

### 7.1.1 - Description

| | |
|---|---|
| **Objectif** | Ces règles visent à garantir l'interopérabilité entre les différents services techniques des administrations. Cela permet à une administration d'utiliser ou d'intégrer dans ses propres applications des services techniques mis à disposition par d'autres administrations, par exemple, accéder à un service d'annuaire, transporter des données ou échanger des fichiers. |
| **Domaine d'interopérabilité** | Intégration entre services techniques |
| **Responsable** | |

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.

### 7.1.2 - Contexte d'introduction du protocole LDAP

Dans le cadre du modèle OSI (*Open Systems Interconnection*) défini par l'ISO, l'UIT a spécifié 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.

### 7.1.3 - 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'administration 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 RGI. Ce projet référence les recommandations RFC 2247 et RFC 2798, à inclure dès à présent au RGI 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 (voir plus loin).

### 7.1.4 - Fonctionnalités

Le protocole LDAP définit les fonctionnalités suivantes :

un protocole réseau pour accéder à l'information contenue dans l'annuaire,
un modèle d'information définissant la forme et le type de l'information contenue dans l'annuaire,
un espace de nommage définissant comment l'information est organisée et référencée,
un modèle fonctionnel définissant comment on accède et met à jour l'information,
un modèle de distribution permettant de répartir les données (à partir de la v3),
un protocole et un modèle de données extensible,
des API pour développer des applications clientes.

### 7.1.5 - Normes et standards applicables

| | |
|---|---|
| RIT0057 | Il est OBLIGATOIRE de prévoir un mode d'accès conforme à LDAP v3 pour les annuaires interrogeables par plusieurs entités administratives. |

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| LDAP V3 | RFC 2251 à 2253 Spécifications du protocole | Proposé | Déc 1997 |
| | RFC 2254 The String Representation of LDAP Search Filters | Proposé | Déc 1997 |
| | RFC 2255 Le format URL pour LDAP | Proposé | Déc 1997 |
| | RFC 2256 A Summary of the X.500 User Schema for use with LDAPv3 | Proposé | Déc 1997 |
| Extensions LDAP | RFC 2798 Classe d'objet inetOrgPerson | Information | Avril 2000 |
| Extensions LDAP | RFC 2247 Utilisation des noms de domaines pour les distinguished names LDAP/X.500 | Proposé | Janv 1998 |
| Messagerie X400 | RFC 2294 Représentation de la hiérarchie d'adresse O/R dans le DIT X500 | Proposé | Mars 1998 |
| Internet X500 | RFC 1274<br>The COSINE and Internet X.500 Schema | Proposé | Nov 1991 |
| X500 URI attribut | RFC 2079 Definition of an X.500 Attribute Type and an Object Class to Hold URI | Proposé | Janv 1997 |
| URI | RFC 2396 Uniform Resource Identifiers | Draft standard | Août 1998 |
| LDAP V3 | RFC 3377 Spécifications techniques | Proposé | Sept 2002 |

### 7.1.6 - Principes de mise en œuvre

*Il n'existe pas encore d'élément référencé.*

### 7.1.7 - Composants

*Il n'existe pas encore d'élément référencé.*

### 7.1.8 - Exemples d'initiatives sectorielles

*Il n'existe pas encore d'élément référencé.*

## 7.2 - Les échanges de données entre annuaires

### 7.2.1 - Description

| | |
|---|---|
| **Objectif** | Ces règles visent à garantir l'interopérabilité entre les différents services techniques des administrations. Cela permet à une administration d'utiliser ou d'intégrer dans ses propres applications des services techniques mis à disposition par d'autres administrations, par exemple, accéder à un service d'annuaire, transporter des données ou échanger des fichiers. |
| **Domaine d'interopérabilité** | Intégration entre services techniques |
| **Responsable** | |

### 7.2.2 - Normes et standards

| | |
|---|---|
| RIT0058 | Il est RECOMMANDÉ d'utiliser le format LDIF pour échanger tout ou partie d'un annuaire de données LDAP. |

**LDAP Data Interchange Format** (LDIF) permet de représenter les données LDAP sous format texte standardisé, il est utilisé pour afficher ou modifier les données de la base. Il a vocation à donner une lisibilité des données à tout utilisateur. LDIF est également utilisé pour importer ou exporter des bases d'informations entre annuaires LDAP.

La majorité des serveurs LDAP supporte ce format ce qui permet une grande interopérabilité entre eux.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| LDIF | RFC 2849 Format d'échanges de données LDAP Spécifications techniques<br><br>http://www.faqs.org/rfcs/rfc2849.html | Proposé | Juin 2000 |

### 7.2.3 - Principes de mise en œuvre

*Il n'existe pas encore d'élément référencé.*

### 7.2.4 - Composants

*Il n'existe pas encore d'élément référencé.*

### 7.2.5 - Exemples d'initiatives sectorielles

*Il n'existe pas encore d'élément référencé.*

## 7.3 - Les extensions pour la sécurité LDAP

### 7.3.1 - Description

| | |
|---|---|
| **Objectif** | Ces règles visent à garantir l'interopérabilité entre les différents services techniques des administrations. Cela permet à une administration d'utiliser ou d'intégrer dans ses propres applications des services techniques mis à disposition par d'autres administrations, par exemple, accéder à un service d'annuaire, transporter des données ou échanger des fichiers. |
| **Domaine d'interopérabilité** | Intégration entre services techniques |
| **Responsable** | |

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.

http://www.iso.org/iso/fr/CatalogueDetailPage.CatalogueDetail?CSNUMBER=20269&ICS1=35&ICS2=100&ICS3=1

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 dans ce document) 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 »).

Certaine 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 frein 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 relatives 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 l'opération en son nom, en tant que client LDAP et en utilisant sa propre identité.

### 7.3.2 - Normes et standards applicables

| | |
|---|---|
| RIT0086 | Il est RECOMMANDÉ d'utiliser les extensions de sécurisation LDAP pour sécuriser les services d'un annuaire de données LDAP. |

| Nom + Version | RFC | Spécification | Etat | Date |
|---|---|---|---|---|
| Extension LDAP | 2649 | Contrôle et schéma LDAP pour les opérations de signature | Expérimental | Aoû-99 |
| | 2820 | Contrôle d'accès pour LDAP | Informationnel | Mai-00 |
| | 2829 | Méthodes d'authentification pour LDAP | Proposé | Mai-00 |
| | 2830 | Extension LDAP v3 pour TLS | Proposé | Mai-00 |
| | 3377 | Spécifications Techniques LDAP v3 | Proposé | Sep-02 |

### 7.3.3 - Principes de mise en œuvre

*Il n'existe pas encore d'élément référencé.*

### 7.3.4 - Composants

*Il n'existe pas encore d'élément référencé.*

### 7.3.5 - Exemples d'initiatives sectorielles

*Il n'existe pas encore d'élément référencé.*

## 7.4 - Autres extensions pour LDAP

### 7.4.1 - Normes et standards à débattre

| Nom + Version | RFC | Spécification | Etat | Date |
|---|---|---|---|---|
| Extensions LDAP | 2927 | Extensions MIME | Informationnel | Sept 2000 |
| idem | 2377 | Extensions pour le nommage Internet | Informationnel | Sept 1998 |
| idem | 2307 | Introduction des entités TCP/IP et Unix | Expérimental | Mars 1998 |
| idem | 1617 | Aide à la définition d'annuaire | Informationnel | Mai 1994 |

# 8 - Interopérabilité des services techniques

## 8.1 - Services de compression de fichiers

### 8.1.1 - Description

| | |
|---|---|
| **Objectif** | Ces règles visent à garantir l'interopérabilité entre les différents services techniques des administrations. Cela permet à une administration d'utiliser ou d'intégrer dans ses propres applications des services techniques mis à disposition par d'autres administrations, par exemple, accéder à un service d'annuaire, transporter des données ou échanger des fichiers. |
| **Domaine d'interopérabilité** | Intégration entre services techniques |
| **Responsable** | |

La compression de données est une technique qui permet de réduire l'espace nécessaire à la représentation d'une certaine quantité d'information. Elle concerne ainsi la transmission des données mais également leurs stockage. Nous de traiterons ici que de la problématique de la compression des fichiers de données.

Les méthodes de compression sont de deux types, les méthodes de compression avec perte et les méthodes de compression sans perte.

### 8.1.2 - Normes et standards

Ce paragraphe est en cours de rédaction.

| | |
|---|---|
| RIT0096 | *En cours de rédaction.* |

### 8.1.3 - Principes de mise en œuvre

*Il n'existe pas encore d'élément référencé.*

### 8.1.4 - Composants

*Il n'existe pas encore d'élément référencé.*

### 8.1.5 - Exemples d'initiatives sectorielles

*Il n'existe pas encore d'élément référencé.*

## 8.2 - Services de noms de domaines

### 8.2.1 - Description

| | |
|---|---|
| **Objectif** | Ces règles visent à garantir l'interopérabilité entre les différents services techniques des administrations. Cela permet à une administration d'utiliser ou d'intégrer dans ses propres applications des services techniques mis à disposition par d'autres administrations, par exemple, accéder à un service d'annuaire, transporter des données ou échanger des fichiers. |
| **Domaine d'interopérabilité** | Intégration entre services techniques |
| **Responsable** | |

### 8.2.2 - Normes et standards

| | |
|---|---|
| RIT0063 | Il est OBLIGATOIRE d'utiliser le service DNS pour accéder aux fonctionnalités de résolution de noms de domaines. |

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

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.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| DNS | RFC 1034 Concepts et fonctionnalités | Standard | Nov. 1987 |
| | RFC 1035 Implémentation et spécifications | Standard | Nov. 1987 |
| | RFC 1101 Actualise les RFC ci-dessus | Non déterminé | Avril 1989 |

## 8.3 - Services sécurisés de noms de domaines

### 8.3.1 - Description

| | |
|---|---|
| **Objectif** | Ces règles visent à garantir l'interopérabilité entre les différents services techniques des administrations. Cela permet à une administration d'utiliser ou d'intégrer dans ses propres applications des services techniques mis à disposition par d'autres administrations, par exemple, accéder à un service d'annuaire, transporter des données ou échanger des fichiers. |
| **Domaine d'interopérabilité** | Intégration entre services techniques |
| **Responsable** | |

### 8.3.2 - Normes et standards

| | |
|---|---|
| RIT0064 | Il est RECOMMANDÉ d'utiliser le service DNSSec pour accéder de manière sécurisée aux fonctionnalités de résolution de noms de domaines. |

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

Or, 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 DNS[2], 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.

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 projets[3] 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).

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

[3] 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.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| DNSSec | RFC 2535 Extensions de sécurité | Proposé standard | Mars 1999 |
| | RFC 2931 Mise à jour de la signature des requêtes et réponses DNS | Proposé standard | Sept. 2000 |
| | RFC 3007 Sécurisation des mises à jour DNS | Proposé standard | Nov. 2000 |
| | RFC 3008 Autorité de signature DNSSec | Proposé standard | Nov. 2000 |

### 8.3.3 - Normes et standards à débattre

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| DNS | RFC 1886 Extensions pour supporter IPv6 | Proposé standard | Déc 1995 |
| DNSSec | RFC 3226 Support des enregistrements DNSSec et des adresses IPv6 | Proposé standard | Déc 2002 |
| DNSSec | RFC 3445 Limitation du champ d'action du Ressource Record KEY | Proposé standard | Déc 2002 |

### 8.3.4 - Principes de mise en œuvre

*Il n'existe pas encore d'élément référencé.*

### 8.3.5 - Composants

*Il n'existe pas encore d'élément référencé.*

### 8.3.6 - Exemples d'initiatives sectorielles

*Il n'existe pas encore d'élément référencé.*

## 8.4 - Services de transfert de fichiers

### 8.4.1 - Description

| | |
|---|---|
| **Objectif** | Ces règles visent à garantir l'interopérabilité entre les différents services techniques des administrations. Cela permet à une administration d'utiliser ou d'intégrer dans ses propres applications des services techniques mis à disposition par d'autres administrations, par exemple, accéder à un service d'annuaire, transporter des données ou échanger des fichiers. |
| **Domaine d'interopérabilité** | Intégration entre services techniques |
| **Responsable** | |

### 8.4.2 - Normes et standards

| | |
|---|---|
| RIT0065 | Il est RECOMMANDÉ, hors contexte Web, d'utiliser le protocole FTP pour réaliser des transferts de fichiers. |
| RIT0066 | Il est INTERDIT d'utiliser le protocole TFTP pour réaliser des transferts de fichiers. |
| RIT0093 | Il est INTERDIT, dans le contexte Web, d'utiliser le protocole FTP pour réaliser des 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 (RFC 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 Général d'Interopérabilité, lorsque requis.

| **Nom + Version** | **Spécification** | **Etat** | **Date** |
|---|---|---|---|
| FTP | RFC 959 Spécifications de base | Standard | Oct 1985 |
| | RFC 2228 Extensions de sécurité | Proposé standard | Oct 1997 |
| | RFC 2640 Extensions aux codes internationaux | Proposé standard | Juill 1999 |
| | RFC 2773 Mécanismes d'encryptage | Expérimental | Fév 2000 |
| | RFC 2389 Négociation des options | Proposé standard | Août 2000 |

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. Par ailleurs, l'utilisation du protocole TFTP (*Trivial File Transfer Protocol*) est totalement proscrite.

## 8.5 - Services de gestion de la qualité de service

### 8.5.1 - Description

| | |
|---|---|
| **Objectif** | Ces règles visent à garantir l'interopérabilité entre les différents services techniques des administrations. Cela permet à une administration d'utiliser ou d'intégrer dans ses propres applications des services techniques mis à disposition par d'autres administrations, par exemple, accéder à un service d'annuaire, transporter des données ou échanger des fichiers. |
| **Domaine d'interopérabilité** | Intégration entre services techniques |
| **Responsable** | |

### 8.5.2 - Principes

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.

### 8.5.3 - Normes et standards

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 champs 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.

## 8.5.4 - Les tendances actuelles

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 (*IntServ*) 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 (*DiffServ*), 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.

## 8.5.5 - Les futurs standards

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

| **Nom + Version** | **Spécification** | **Etat** | **Date** |
|---|---|---|---|
| RSVP (IntServ) | RFC 2205 Spécifications fonctionnelles | Proposé standard | Sept 1997 |
| DiffServ | RFC 2474 Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers | Proposé standard | Déc 1998 |
| | RFC 2597 Assured Forwarding PHB Group | Proposé standard | Juin 1999 |
| | RFC 2598 An Expedited Forwarding PHB | Proposé standard | Juin 1999 |

## 8.6 - Services de gestion des NewsGroups

### 8.6.1 - Description

| | |
|---|---|
| **Objectif** | Ces règles visent à garantir l'interopérabilité entre les différents services techniques des administrations. Cela permet à une administration d'utiliser ou d'intégrer dans ses propres applications des services techniques mis à disposition par d'autres administrations, par exemple, accéder à un service d'annuaire, transporter des données ou échanger des fichiers. |
| **Domaine d'interopérabilité** | Intégration entre services techniques |
| **Responsable** | |

### 8.6.2 - Normes et standards

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.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| NNTP | RFC 977<br>Spécification du protocole | Proposé standard | Fév 1986 |

### 8.6.3 - Principes de mise en œuvre

*Il n'existe pas encore d'élément référencé.*

### 8.6.4 - Composants

*Il n'existe pas encore d'élément référencé.*

### 8.6.5 - Exemples d'initiatives sectorielles

*Il n'existe pas encore d'élément référencé.*

## 8.7 - Le format URI d'identification des ressources Internet

### 8.7.1 - Description

| | |
|---|---|
| **Objectif** | Ces règles visent à garantir l'interopérabilité entre les différents services techniques des administrations. |
| **Domaine d'interopérabilité** | Intégration entre services techniques |
| **Responsable** | |

### 8.7.2 - Normes et standards

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.internet.gouv.fr signifie que l'on cherche à atteindre, via le protocole HTTP, les ressources Web du portail « Société de l'information-Internet » sous l'arborescence gouvernement du pays France.

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'administration 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 Général d'Interopérabilité.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| URI | RFC 2396 | Draft standard | Août 1998 |

### 8.7.3 - Principes de mise en œuvre

*Il n'existe pas encore d'élément référencé.*

### 8.7.4 - Composants

*Il n'existe pas encore d'élément référencé.*

### 8.7.5 - Exemples d'initiatives sectorielles

Service de Méta Annuaire Inter Administration (MAIA)

http://annuaire.ader.gouv.fr/

# 9 - Interopérabilité et Sécurisation des échanges

| | |
|---|---|
| **Objectif** | Ces règles s'adressent aux architectes et chefs de projet responsables de la mise en place d'échanges entre administrations. La normalisation des formats d'échange est particulièrement importante pour permettre :<br>1. L'émergence de dispositifs de signature 'off-line', ce qui est nécessaire pour les environnements de faible connectivité (zones blanches) ou pour les applications à forte mobilité,<br>2. L'intégration dans des applications métiers (comme par exemple l'envoi depuis les logiciels de gestion des délibérations des actes soumis au contrôle de légalité),<br>3. L'utilisation de passerelles de l'administration électronique.<br>Une réflexion est actuellement en cours pour le choix du modèle d'échange à mettre en place.<br>Ces règles décrivent les solutions permettant d'assurer la sécurité des échanges entre les administrations tout en garantissant l'interopérabilité entre les différents composants. Par exemple, une administration peut transférer des informations concernant des usagers en voulant garantir la confidentialité de ces informations |
| **Domaine d'interopérabilité** | • Intégration des services de sécurité,<br>• Accès aux services en ligne,<br>• Intégration entre portails,<br>• Intégration entre portails et téléservices,<br>• Intégration entre portails et services administratifs,<br>• Intégration entre téléservices,<br>• Intégration entre services techniques,<br>• Intégration entre téléservices et services techniques. |
| **Responsable** | |

## 9.1 - Protocoles d'échanges de messages

### 9.1.1 - Description

Pour faire suite à un appel à commentaires, lancé en 2005, un groupe de travail a été constitué. Animé par la DGME, ce groupe est actuellement en phase de définition du protocole d'échange de l'administration électronique. Ce protocole appelé PRESTO aura pour rôle de véhiculer les messages entre les différents acteurs concernés par l'Ordonnance n° 2005-1516 sur les échanges électroniques, et éventuellement les administrations européennes.

### 9.1.2 - Normes et standards

| | |
|---|---|
| RIT0067 | Il est apparu nécessaire de disposer au sein de l'administration d'un protocole d'échanges de messages. Une règle sera édictée dès que le protocole sera disponible. |

Ce protocole concerne donc les échanges entre acteurs de l'administration électronique et n'a pas vocation à régir les échanges internes de chaque système d'information. Des démonstrateurs seront disponibles aux besoins de l'administration vers mi-2006.

Si les travaux du consortium WS-I amènent à la publication d'une spécification « Web Services Basic Profile V2.0 », dont le contenu serait en convergence avec le protocole d'échange de l'administration électronique, alors le RGI recommanderait d'utiliser cette spécification.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| PRESTO | Protocole d'échanges entre acteurs de l'administration électronique | En cours d'élaboration | 2006 |

## 9.1.3 - Principes de mise en œuvre

*Il n'existe pas encore d'élément référencé.*

## 9.1.4 - Composants

*Il n'existe pas encore d'élément référencé.*

## 9.1.5 - Exemples d'initiatives sectorielles

- Programme Européen : Norme IDA (« Interchange of Data between Administrations ») eLink v2

  http://europa.eu.int/idabc/en/document/3489/5585

- Caisse des Dépôts et des Consignations : Norme FAST v1.1.

  http://www.fast.caissedesdepots.fr/

- 0Consortium OASIS (Organization for the Advancement of Structured Information Standards): protocole ebMS2 utilisé dans le cadre d'échanges ebXML (electronic business XML). La version 3 devrait se rapprocher des standards émergeants liés aux Web Services.

  http://www.ebxml.org/specs/ebMS2.pdf

- Le Protocole d'Echanges Standard (PES) du MINEFI :

  Présentation technique générale du PES.

  Spécifications fonctionnelles et techniques pour la mise en œuvre du PES.

  http://www.colloc.minefi.gouv.fr/

## 9.2 - Services de sécurisation des échanges

### 9.2.1 - Description

**Transport Layer Security** (TLS), anciennement nommé Secure Socket Layer (SSL) est un protocole de sécurisation des échanges sur Internet, développé à l'origine par la société Netscape (SSL versions 2 et 3). Il a été renommé en Transport Layer Security (TLS) par l'IETF suite au rachat du brevet de Netscape par l'IETF en 2001. Le groupe de travail correspondant à l'IETF a permis la création de la RFC 2246.

Il y a très peu de différence entre SSL version 3 et TLS version 1 (qui correspond à la version 3.1 du protocole SSL) rendant les deux protocoles non interopérables, mais TLS a mis en place un mécanisme de compatibilité ascendante avec SSL. En outre, TLS diffère de SSL pour la génération des clés symétriques. Cette génération est plus sécurisée dans TLS que dans SSL v3 dans la mesure où aucune étape de l'algorithme ne repose uniquement sur MD5 pour lequel sont apparues quelques faiblesses en cryptanalyse.

Par abus de langage, on parle de SSL pour désigner indifféremment SSL ou TLS. SSL fonctionne suivant un mode client/serveur. Il fournit quatre objectifs de sécurité :

l'authentification du serveur;
la confidentialité des données échangées (ou session chiffrée);
l'intégrité des données échangées
de manière optionnelle, l'authentification du client.

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

pour toutes applications existantes, il peut exister une application utilisant SSL. Par exemple, l'application HTTPS correspond à HTTP au dessus de SSL;

une application SSL se voit attribuer un nouveau numéro de port par l'IANA. Par exemple HTTPS est associé au port 443.

**Secure Socket Layer** (SSL) est un protocole de communication sécurisé qui propose plusieurs services de sécurité :

Authentification des parties communicantes par utilisation de certificats X.509 v3 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 dés 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 présentation, 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.

## 9.2.2 - Normes et standards

| | |
|---|---|
| RIT0068 | Il est RECOMMANDÉ d'utiliser les protocoles TLS 1.0 et SSL 3.0 pour sécuriser les échanges utilisant les protocoles HTTP, LDAP, FTP, etc. |

TLS est un protocole permettant d'ajouter une couche de sécurité à des protocoles existants comme par exemple HTTP (protocole HTTPS), LDAP (protocole LDAPS), FTP (protocole Secure FTP) …

TLS fournit des fonctions d'authentification (client et serveur), de chiffrement et de garantie d'intégrité. TLS a été standardisé par l'IETF à partir de la norme SSL 3.0 définie par Netscape.

| **Nom + Version** | **Spécification** | **Etat** | **Date** |
|---|---|---|---|
| TLS 1.0 | RFC 2246 Spécifications du protocole | Proposé standard | Janv 1999 |
| SSL 3.0 | http://wp.netscape.com/eng/ssl3/ | Draft | Nov 1996 |
| FTP | RFC 2228 Extensions de sécurité | Proposé standard | Oct 1997 |
| FTP | RFC 4217 Securiser FTP avec TLS | Proposé standard | Oct 2005 |

## 9.2.3 - Principes de mise en œuvre

*Il n'existe pas encore d'élément référencé.*

## 9.2.4 - Composants

*Il n'existe pas encore d'élément référencé.*

## 9.2.5 - Exemples d'initiatives sectorielles

*Il n'existe pas encore d'élément référencé.*

## 9.3 - Services de chiffrement des documents XML

### 9.3.1 - Description

XML Encryption est un protocole développé par le W3C qui décrit le principe de chiffrement d'un contenu numérique. Le standard XML Encryption inclus des protocoles pour chiffrer les sections des documents XML.

XLM 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.

XLM Encryption permet de chiffrer l'ensemble ou une partie d'un document XML et représenter le résultat sous forme XML.

### 9.3.2 - Normes et standards

| | |
|---|---|
| RIT0069 | Il est RECOMMANDÉ d'utiliser le protocole XMLENC pour chiffrer des documents XML. |

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| XMLENC | http://www.w3.org/TR/xml-encryption-req<br>(XML Encryption Requirements) | « Draft » W3C | déc 2002 |
| | http://www.w3.org/TR/xml-encryption-req<br>(XML Encryption Syntax and Processing) | « Draft » W3C | déc 2002 |
| | http://www.w3.org/TR/xmlenc-decrypt<br>(Decryption Transform for XML Signature) | « Draft » W3C | déc 2002 |

### 9.3.3 - Principes de mise en œuvre

*Il n'existe pas encore d'élément référencé.*

### 9.3.4 - Composants

*Il n'existe pas encore d'élément référencé.*

### 9.3.5 - Exemples d'initiatives sectorielles

*Il n'existe pas encore d'élément référencé.*

## 9.4 - Services de signature des documents XML

### 9.4.1 - Description générale

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'une 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, le protocole 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 XLM peut également s'appliquer à plusieurs types de ressource en même temps. Par exemple, une seule signature XML peut couvrir des données HTML, une image JPEG, des 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 Ressource 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.

### 9.4.2 - Description détaillée

XAdES (XML Advanced Electronic Signature) ETSI TS 101 903 est une norme définie par l'ETSI (European Telecommunications Standards Institute).

XAdES s'appuie sur la recommandation XML DSIG qui a été définie par le Groupe XML-Signature Working Group du W3C à l'IETF. XML DSIG permet de signer des documents XML ou des parties de document afin de garantir leur intégrité et d'authentifier l'entité ayant signé le document.

L'objectif de XAdES est :

- de répondre au besoin de validité de la signature sur le long terme;
- de répondre aux exigences de la directive européenne sur la signature électronique.

Cela est réalisé par :

- des fonctions de non répudiation et d'horodatage;
- l'ajout d'informations à la signature pour prendre en charge des cas d'utilisation classiques.

### 9.4.3 - Normes et standards

| | |
|---|---|
| RIT0070 | Il est OBLIGATOIRE d'utiliser la fonction de signature XAdES pour signer des documents XML. |

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| XAdES | XML Advanced Electronic Signature<br><br>http://uri.etsi.org/01903/v1.1.1/<br><br>http://uri.etsi.org/01903/v1.1.1/ts_101903v010101p.pdf | publiée | Fév 2002 |
| | http://www.w3.org/TR/XAdES/ | Note | Fév 2003 |
| | Profil de signature XAdES pour l'administration électronique.<br>http://www.adae.gouv.fr/article.php3?id_article=1035&var_recherche=xades | publié | Mai 2006 |
| XMLDSIG | http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/ | Recommandation W3C | Fév 2002 |
| | RFC 2807 Préconisations pour la signature XML | Informationnel | Juillet 2000 |
| | RFC 3275<br>Syntaxe et mise en œuvre de la signature XML | Proposé | Mars 2002 |

### 9.4.4 - Principes de mise en œuvre

*Il n'existe pas encore d'élément référencé.*

### 9.4.5 - Composants

*Il n'existe pas encore d'élément référencé.*

### 9.4.6 - Exemples d'initiatives sectorielles

*Il n'existe pas encore d'élément référencé.*

## 9.5 - Services de sécurisation des «Web Services»

### 9.5.1 - Description

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 multicanaux) 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) est un pas énorme dans la capacité à intégrer des processus applicatifs. Ceci est fait 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, émergeants 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. On peut citer notamment WS-Security, qui apporte un support global de l'intégrité, de la confidentialité et de l'authentification des messages. On peut citer aussi SAML, qui définit un langage commun d'interopérabilité permettant de décrire et partager des informations liées à l'authentification et l'autorisation. Ceci facilite la mise en place de fonctionnalités SSO et permet la délégation de droits. D'autres propositions émergentes, telles que XKMS ou XACML viennent compléter les manques en matière de sécurité.

### 9.5.2 - Normes et standards

| | |
|---|---|
| RIT0071 | Il est RECOMMANDÉ d'utiliser la fonction WS-Security pour sécuriser des Web Services. |

WS-Security décrit un mécanisme permettant de sécuriser les Web Services. Les domaines couverts concernent l'intégrité, la confidentialité et l'authentification. Ce standard décrit en particulier l'utilisation des certificats X.509 et des tickets Kerberos. Aujourd'hui peu de produits mettent en œuvre ce standard.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| WS-Security V1.1 | http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss | Standard Oasis | Fév 2006 |

## 9.6 - Services de gestion de clés pour «Web Services»

### 9.6.1 - Description

XKMS (XML Key Manipulation Service) est une composante de la plate-forme Web Services qui permet développeurs de sécuriser les échanges en s'appuyant sur une PKI. Le service XKMS est une spécification importante 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 concentre 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 plates-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.

### 9.6.2 - Normes et standards

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| XKMS | Spécifications XKMS 2.0 - http://www.w3.org/TR/xkms2/ | Document de travail W3C | Mars 2002 |
| | Exigences XKMS - http://www.w3.org/TR/xkms2-req | Document de travail W3C | Mars 2002 |

### 9.6.3 - Principes de mise en œuvre

*Il n'existe pas encore d'élément référencé.*

### 9.6.4 - Composants

*Il n'existe pas encore d'élément référencé.*

### 9.6.5 - Exemples d'initiatives sectorielles

*Il n'existe pas encore d'élément référencé.*

## 9.7 - Services de contrôle d’accès aux ressources XML

### 9.7.1 - Description

XACML (eXtensible Access Control Markup Language) est une spécification de l’OASIS qui est utilisée conjointement avec SAML (voir également dans ce chapitre) 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 un 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 un endroit physiquement séparé du document XML, endroit auquel il est fait référence lors de la requête. XPointers et XPaths 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.

### 9.7.2 - Normes et standards

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| XACML | Spécifications XACML<br><br>http://www.oasis-open.org/committees/xacml/repository/cs-xacml-specification-01.pdf | Spécifications OASIS | Déc 2002 |

### 9.7.3 - Principes de mise en œuvre

*Il n'existe pas encore d'élément référencé.*

### 9.7.4 - Composants

*Il n'existe pas encore d'élément référencé.*

### 9.7.5 - Exemples d'initiatives sectorielles

*Il n'existe pas encore d'élément référencé.*

## 9.8 - Protocole de déclaration de données utilisateur

### 9.8.1 - Description

SAML (Security Assertion Markup Language) est un protocole de déclaration de données d'authentification et d'autorisation. Il est développé par le W3C. La spécification SAML 1.0 est issue de la fusion de deux anciens travaux concurrents S2ML et AUthML. 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.

La spécification SAML 2.0 a été présentées à l'OASIS en mars 2005.

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. C'est le principe du Single Sign On.

L'idée de services de SSO n'est pas nouvelle et des solutions propriétaires existent depuis des années mais elles offrent peu ou pas 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.

### 9.8.2 - Normes et standards

| | |
|---|---|
| RIT0090 | Il est RECOMMANDÉ d'utiliser le langage SAML v2.0 (Security Assertion Markup Language) pour les déclarations de données d'authentification et d'autorisation. |

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| SAML 1.0 | Définition du langage http://www.oasis-open.org/committees/security/docs/cs-sstc-core-01.pdf | Standard OASIS | Mai 2002 |
| | Règles d'interfaçage avec SAML http://www.oasis-open.org/committees/security/docs/cs-sstc-bindings-01.pdf | Standard OASIS | Mai 2002 |
| | 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 | Standard OASIS | Mai 2002 |
| | Programme de conformité à SAML http://www.oasis-open.org/committees/security/docs/cs-sstc-conform-01.pdf | Standard OASIS | Mai 2002 |
| SAML 2.0 | Définition du langage<br><br>http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf | Standard OASIS | Mars 2005 |

## 9.9 - Invocation de services

### 9.9.1 - Description

| | |
|---|---|
| **Objectif** | Ces règles s'adressent aux architectes et développeurs de services administratifs, de téléservices et de services techniques.<br>Elles visent à garantir l'interopérabilité entre ces différents composants. Cela permet à une administration d'utiliser ou d'intégrer dans ses propres applications des services mis à disposition par d'autres administrations.<br>Par exemple, un téléservice de saisie de changement d'adresse peut s'appuyer sur un service de validation d'adresses géopostales mis à disposition par une autre administration ou un partenaire externe. |
| **Domaine d'interopérabilité** | • Intégration entre portails et téléservices,<br>• Intégration entre portails et services administratifs,<br>• Intégration entre services techniques,<br>• Intégration entre téléservices et services techniques. |
| **Responsable** | |

### 9.9.2 - Normes et standards

Les Web Services décrivent un moyen de publier des traitements de manière normalisée et de les rendre accessibles à des traitements distants de manière indépendante des technologies utilisées. Les Web Services doivent échanger des messages au format SOAP.

| | |
|---|---|
| RIT0059 | Il est RECOMMANDÉ de s'appuyer sur le protocole SOAP 1.1 lors de la conception de Web Services. |

Simple Object Access Protocol (SOAP) est un protocole d'appel de procédures à distance. Il est orienté objet et bâti sur le langage XML. Il permet la transmission de messages entre objets distants, ce qui signifie qu'il autorise un objet à invoquer des méthodes d'objets physiquement situés sur une autre machine. Le transport des données est réalisé le plus souvent à l'aide du protocole HTTP, mais peut également se faire par un autre protocole, comme SMTP.

Le protocole SOAP est composé de deux parties, une enveloppe, contenant des informations sur le message lui-même et un modèle de données, définissant le format du message.

Défini à l'origine par Microsoft et IBM, SOAP est devenu depuis une recommandation du W3C, utilisée notamment dans le cadre d'architectures de type SOA pour les Web Services.

**Remarque** : dans le cas particulier des services relatifs à la fédération d'identité, il est obligatoire d'utiliser SOAP 1.1 tel que décrit dans les spécifications Liberty Alliance ID-FF 1.2. Par ailleurs pour rester cohérent avec Web Services Basic Profile V1.0, il faut retenir SOAP 1.1 d'où la règle énoncée.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| SOAP 1.1 | http://www.w3.org/TR/2000/NOTE-SOAP-20000508/ | Recommandation W3C | Mai 2000 |
| SOAP 1.2 | http://www.w3.org/TR/soap<br><br>http://www.w3.org/2002/ws | Recommandation W3C | Juin 2003 |

| | |
|---|---|
| RIT0091 | Il est OBLIGATOIRE de dissocier la couche Web Services de la couche de transport (HTTP, SMTP, ...). |

La couche permettant de transporter des Web Services peut-être assurée par des protocoles autres que HTTP comme par exemple SMTP.

| | |
|---|---|
| RIT0060 | Il est OBLIGATOIRE de décrire les interfaces des services exposés à l'aide de documents à la norme WSDL. |

Tout fournisseur de service doit fournir aux utilisateurs de ce service (autres administrations, partenaires externes ...) une description du service conforme à la norme WSDL.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| WSDL 1.1 | http://www.w3.org/TR | Note | Mars 2001 |
| RFC 2965 | HTTP State Management Mechanism | Standard | oct 2000 |

UDDI (Universal Description Discovery and Integration) permet d'implémenter des annuaires permettant de localiser des Web Services. C'est une technologie d'annuaire basée sur XML et plus particulièrement destinée aux services web, notamment dans le cadre d'architectures de type SOA. Un annuaire UDDI permet de localiser sur le réseau le service Web recherché. Il repose sur le protocole de transport SOAP.

Il n'y a pas de règle d'interopérabilité sur ce sujet pour l'instant.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| UDDI | http://www.oasis-open.org/committees/uddi-spec/doc/tcspecs.htm<br><br>http://www.uddi.org/ | Standard | |
| UDDI V3 | http://www.oasis-open.org/committees/uddi-spec/doc/tcspecs.htm#uddiv3 | Standard | Oct 2004 |

## 9.9.3 - Principes de mise en œuvre

| | |
|---|---|
| RIT0062 | Il est RECOMMANDÉ de se conformer au profil d'utilisation des Web Services « Basic Profile 1.0 ». |

La spécification « Basic Profile » définit un ensemble de règles concernant l'utilisation des Web Services permettant de favoriser l'interopérabilité. Elle a été définie par le consortium WS-I, « Web Services Interoperabilty Organisation ».

Ces règles concernent les points suivants :

- Messages : encodage, représentation des données, gestion des erreurs,
- Description des Web Services : utilisation de WSDL,
- Découverte des Web Services : UDDI, utilisation de méta-données,
- Sécurité : utilisation de HTTPS et des certificats X.509.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| Web Services Basic Profile V1.0 | http://www.ws-i.org/deliverables/workinggroup.aspx?wg=basicprofile | Final | 16 avril 2004 |
| Web Services Basic Profile V1.1 | http://www.ws-i.org/Profiles/BasicProfile-1.1-2004-08-24.html | | Août 2004 |

## 9.9.4 - Composants

*Il n'existe pas encore d'élément référencé.*

## 9.9.5 - Exemples d'initiatives sectorielles

*Il n'existe pas encore d'élément référencé.*

# 10 - Interopérabilité des protocoles

## 10.1 - Le Protocole IP (couche réseau)

### 10.1.1 - Description

| | |
|---|---|
| **Objectif** | Ces règles visent à garantir l'interopérabilité entre les différents services techniques des administrations. Cela permet à une administration d'utiliser ou d'intégrer dans ses propres applications des services techniques mis à disposition par d'autres administrations, par exemple, accéder à un service d'annuaire, transporter des données ou échanger des fichiers. |
| **Domaine d'interopérabilité** | Intégration entre services techniques |
| **Responsable** | |

### 10.1.2 - Normes et standards

| | |
|---|---|
| RIT0075 | Il est OBLIGATOIRE d'utiliser le protocole IP V4 pour l'ensemble des échanges au niveau de la couche réseau. |

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 (exemple : 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. La question de l'adoption de cette orientation se pose donc tant en terme de délai de mise en œuvre, qu'en terme de coût de la migration. L'évolution du marché décidera du moment opportun (croissance du réseau, développement de l'Internet mobile de masse, du multimédia, …).

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 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 (exemple : 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 émergeant.

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 proposée antérieurement, est toujours d'actualité. Il est donc conseillé de reconduire le référentiel à l'identique pour la présente version 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 Koctets, 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 Koctets 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 dans un but de suivi et de veille technologique.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| IP V4 | RFC 791<br>Spécification du protocole | Standard | Sept 1981 |

### 10.1.3 - Evolution du protocole

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

| Nom + Version | RFC | Spécification | Etat | Date |
|---|---|---|---|---|
| IPv6 | 2373 | Architecture d'adressage IP V6 | Proposé standard | Juill 1998 |
| | 2374 | Format d'adressage unicast IP V6 | Proposé standard | Juill 1998 |
| | 2460 | Spécification du protocole | Draft standard | déc 1998 |
| | 2461 | Découverte de l'environnement | Draft standard | déc 1998 |
| | 2462 | Autoconfiguration | Draft standard | déc 1998 |
| | 2463 | ICMP V6 | Draft standard | déc 1998 |
| IP V6 TCP/UDP | 2675 | Augmentation du volume des paquets | Proposé standard | Août 1999 |
| Transition IP.V4 -> IP.V6 | 2893 | Mécanisme de transition | Proposé standard | Août 2000 |
| Transition IP.V4 -> IP.V6 | 2766 | NAT-PT pour IP v6 | Proposé standard | Fév 2000 |

### 10.1.4 - Principes de mise en œuvre

*Il n'existe pas encore d'élément référencé.*

### 10.1.5 - Composants

*Il n'existe pas encore d'élément référencé.*

### 10.1.6 - Exemples d'initiatives sectorielles

*Il n'existe pas encore d'élément référencé.*

## 10.2 - Le Protocole IPSEC (couche réseau)

### 10.2.1 - Description

| | |
|---|---|
| **Objectif** | Ces règles visent à garantir l'interopérabilité entre les différents services techniques des administrations. Cela permet à une administration d'utiliser ou d'intégrer dans ses propres applications des services techniques mis à disposition par d'autres administrations, par exemple, accéder à un service d'annuaire, transporter des données ou échanger des fichiers. |
| **Domaine d'interopérabilité** | Intégration entre services techniques |
| **Responsable** | |

IPSEC est un protocole qui assure l'authentification, le chiffrement des données et l'intégrité. Contrairement à TLS qui est spécifié au niveau de la couche présentation, IPSEC est définie au niveau IP (couche réseau). Il permet par exemple de réaliser des VPN (Virtual Private Network) traduit en Français par réseau privé virtuel.

Un réseau privé virtuel IPsec consiste à établir deux canaux de communication entre les machines :

un canal d'échange de clés, sur une connexion UDP depuis et vers le port 500 (*ISAKMP* pour *Internet Security Association and Key Management Protocol*), défini dans la RFC 2408,

un ou plusieurs canaux de données par lesquels le trafic du réseau privé est véhiculé, deux protocoles sont possibles :

* le protocole IP n°50 *ESP* (*Encapsulating Security Payload*), défini dans la RFC 2406 qui fournit l'intégrité et la confidentialité,
* *AH* (*Authentication Header*) qui ne fournit que l'intégrité, il est spécifié dans la RFC 2402.

La mise en place d'une architecture sécurisée à base d'IPSEC est détaillée dans la RFC 2401.

### 10.2.2 - Normes et standards

| | |
|---|---|
| RIT0076 | Il est RECOMMANDÉ d'utiliser le protocole IPSEC pour encrypter les échanges au niveau de la couche réseau. |

| Nom + Version | RFC | Spécification | Etat | Date |
|---|---|---|---|---|
| IPSEC | RFC 2401 à 2410 | Architecture de sécurité | Proposé standard | nov 1998 |
| | RFC 2411 | Description générale | Informationnel | nov 1998 |
| | RFC 2412 | Protocole OAKLEY | Informationnel | nov 1998 |

## 10.3 - Les Protocoles TCP et UDP (couche transport session)

### 10.3.1 - Description

| | |
|---|---|
| **Objectif** | Ces règles visent à garantir l'interopérabilité entre les différents services techniques des administrations. Cela permet à une administration d'utiliser ou d'intégrer dans ses propres applications des services techniques mis à disposition par d'autres administrations, par exemple, accéder à un service d'annuaire, transporter des données ou échanger des fichiers. |
| **Domaine d'interopérabilité** | Intégration entre services techniques |
| **Responsable** | |

### 10.3.2 - Normes et standards

| | |
|---|---|
| RIT0077 | Il est OBLIGATOIRE d'utiliser les protocoles TCP (Transmission Control Protocol) et UDP (User Datagram Protocol) pour transporter les flux provenant des couches applicatives. |

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.

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.

| Nom + Version | RFC | Spécification | Etat | Date |
|---|---|---|---|---|
| UDP | 768 | Spécification du protocole | Standard | Août 1980 |
| TCP | 793 | Spécification du protocole | Standard | Sept 1981 |
| TCP | 1323 | Extensions pour le haut débit | Proposé standard | Mai 1992 |

## 10.3.3 - Evolutions des standards

Les futures recommandations à intégrer au RGI 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.

| Nom + Version | RFC | Spécification | Etat | Date |
|---|---|---|---|---|
| TCP | 2018 | Acquittement sélectif des données | Proposé standard | Oct 1996 |
| TCP | 2581 | Contrôle de congestion (mis à jour par la RFC 3390) | Proposé standard | Avril 1999 |
| TCP | 2873 | Gestion de la priorité IPv4 | Proposé standard | Juin 2000 |
| TCP | 2883 | Extension à l'acquittement sélectif | Proposé standard | Juil 2000 |
| TCP | 3042 | Nouveau mécanisme pour améliorer la gestion de perte de données | Proposé standard | Janv 2001 |
| TCP | 3168 | Notification explicite de congestion | Proposé standard | Sept 2001 |
| TCP | 3390 | Augmentation de la fenêtre initiale | Proposé standard | Oct 2002 |
| IPv6 TCP/UDP | 2675 | Augmentation du volume des paquets (voir le chapitre sur le protocole IP) | Proposé standard | Août 1999 |

## 10.3.4 - Principes de mise en œuvre

Chaque protocole est mieux adapté que l'autre sur certains domaines.

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

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

## 10.3.5 - Composants

*Il n'existe pas encore d'élément référencé.*

## 10.3.6 - Exemples d'initiatives sectorielles

*Il n'existe pas encore d'élément référencé.*

## 10.4 - Le protocole HTTP (niveau présentation application)

### 10.4.1 - Description

| | |
|---|---|
| **Objectif** | Ces règles visent à garantir l'interopérabilité entre les différents services techniques des administrations. Cela permet à une administration d'utiliser ou d'intégrer dans ses propres applications des services techniques mis à disposition par d'autres administrations, par exemple, accéder à un service d'annuaire, transporter des données ou échanger des fichiers. |
| **Domaine d'interopérabilité** | Intégration entre services techniques |
| **Responsable** | |

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

### 10.4.2 - Normes et standards

| | |
|---|---|
| RIT0078 | Il est RECOMMANDÉ d'utiliser le protocole HTTP 1.1 (HyperText Transfer Protocol) pour la présentation et les échanges entre un serveur Web et un navigateur. |

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| HTTP 1.1 | RFC 2616 Spécifications du protocole | Draft standard | Juin 1999 |
| | RFC 2817 Upgrading to TLS Within HTTP/1.1 | Proposé standard | Mai 2000 |
| | URIs, Addressability, and the use of HTTP GET and POST http://www.w3.org/2001/tag/doc/whenToUseGet.html | Approuvé par le «Technical Architecture Group» | Mars 2004 |

### 10.4.3 - Principes de mise en œuvre

| | |
|---|---|
| RIT0079 | Il est OBLIGATOIRE d'utiliser la méthode HTTP POST au lieu de la méthode HTTP GET lors du passage de paramètres autres que les identifiants de session. |

HTTP en version 1.1 définit officiellement 47 directives (ou en-tête). La directive « Allow » détermine la méthode utilisée (GET, PUT, POST, ...) pour accéder aux ressources demandées.

La méthode GET est la plus simple car le corps du message dans ce type de requête est vide. La méthode POST permet d'envoyer des informations au serveur dans le corps du message d'une requête HTTP. Lorsque des informations sont envoyées au serveur à l'aide de la méthode GET, elles sont encodées à la suite de la ressource après le symbole '?' dans l'url.

Le passage de paramètres par la méthode GET est dépendant du navigateur ; c'est pour cette raison que cette méthode est interdite dans le cadre du RGI.

## 10.5 - Le protocole NTP (Network Time Protocol)

### 10.5.1 - Description

| | |
|---|---|
| **Objectif** | Ces règles visent à garantir l'interopérabilité entre les différents services techniques des administrations. Cela permet à une administration d'utiliser ou d'intégrer dans ses propres applications des services techniques mis à disposition par d'autres administrations, par exemple, accéder à un service d'annuaire, transporter des données ou échanger des fichiers. |
| **Domaine d'interopérabilité** | Intégration entre services techniques<br>Horodatage |
| **Responsable** | |

### 10.5.2 - Normes et standards

| | |
|---|---|
| RIT0080 | Il est RECOMMANDÉ d'utiliser le protocole NTP pour réaliser une synchronisation des horloges des différents ordinateurs et équipements réseaux constituant un Système d'Information. |

Le NTP est un protocole permettant de synchroniser l'horloge d'un ordinateur avec celle d'un serveur de référence. NTP est un protocole basé sur UDP.

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| NTP V3 | RFC 1305 Network Time Protocol<br>http://www.faqs.org/rfcs/rfc1305.html | Draft Standard | Oct 1992 |
| NTP V4 | Evolution de NTP non formalisée dans un RFC<br>http://www.ntp.org/ | | |

| | |
|---|---|
| RIT0081 | Il est RECOMMANDÉ d'utiliser les signaux horaires DCF77 pour d'obtenir une fonction d'horodatage précise. |

La réception des horaires DCF77 est le seul moyen en Europe d'obtenir une heure précise, de manière fiable, avec un récepteur simple (la réception de signaux horaires provenant de satellites GPS est plus difficile à mettre en oeuvre). On peut ainsi recevoir l'heure, la date, et le jour de la semaine. Le changement entre l'heure d'été et d'hiver est automatique. L'émetteur des signaux horaires DCF77 est situé en Allemagne, près de Francfort. Le signal proprement dit est constitué d'une porteuse de 77.5 KHz. L'information horaire est donnée par l'horloge atomique de l'Institut de physique et de métrologie de Brunswick. Cette horloge est très précise, puisque son écart théorique est de ±1 seconde pour 1 millions d'années.

Pour les DOM et les TOM, la mise en œuvre de système utilisant la réception de signaux horaires provenant de satellites GPS ou de futurs satellites Galiléo est recommandée.

## 10.6 - Les protocoles de Voix et de Téléphonie sur IP

### 10.6.1 - Description

| | |
|---|---|
| **Objectif** | Ces règles visent à garantir l'interopérabilité entre les différents services techniques des administrations. Cela permet à une administration d'utiliser ou d'intégrer dans ses propres applications des services techniques mis à disposition par d'autres administrations, par exemple, accéder à un service d'annuaire, transporter des données ou échanger des fichiers. |
| **Domaine d'interopérabilité** | Intégration entre services techniques<br>Intégration voix données<br>Couplage téléphonie informatique |
| **Responsable** | |

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

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

La téléphonie sur IP et le couplage téléphonie informatique (CTI), sont des technologies qui, combinées ensemble, pourraient être utilisées dans le cas de guichet à distance ou de guichet virtuel. Il ne faut pas oublier que les offres ADSL TriplePlay et même QuadruplePlay se répandent très vite chez les usagers (particuliers ou petites structures).

### 10.6.2 - Normes et standards de signalisation

Les principaux protocoles utilisés pour l'établissement de sessions de communication en voix sur IP sont :

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| H.323 | Recommandation H.323<br>Systèmes et équipements visiophoniques pour réseaux locaux offrant une qualité de service non garantie.<br><br>http://www.itu.int/ITU-T/ | Norme approuvée (dernière révision en jan 2005) | Nov 1996 |
| MGCP V1 | Media Gateway Control Protocol<br>RFC 2705<br>http://www.ietf.org/rfc/rfc2705.txt | Informationnel | Oct 1999 |
| SIP V2 | Session Initiation Protocol<br>RFC 3261<br>http://www.ietf.org/rfc/rfc3261.txt | Proposed Standard | Juin 2002 |

MGCP est l'acronyme de Media Gateway Control Protocol. C'est un protocole développé par Telcordia et Level 3 Communications et dont les spécifications sont rendues publiques dans le RFC 2705. MGCP est un protocole asymétrique de type « client-serveur » de VoIP (Voix sur réseau IP). Il se distingue des protocoles SIP et H323 qui, eux, sont symétriques (client-client).

SIP est l'acronyme de Session Initiation Protocol. C'est un protocole normalisé et standardisé par l'IETF et dont les spécifications sont rendues publiques dans le RFC 3261. SIP a été conçu pour établir, modifier et terminer des sessions de communication multimédia. Il est plus récent et moins lourd que le protocole H.323.

Ces protocoles sont de niveau Session (modèle OSI couche 5).

http://www.cndp.fr/notestech/39/nt039_C.htm

## 10.6.3 - Normes et standards de transport

Les principaux protocoles utilisés pour le transport sur IP de la voix elle-même sont :

| Nom + Version | Spécification | Etat | Date |
|---|---|---|---|
| RTP | Real-time Transport Protocol<br>RFC 3550 | Standard | Juill 2003 |
| RTCP | RTP Control Protocol<br>(intégré dans RTP) | | |

Ces protocoles sont de niveau Transport (modèle OSI couche 4) mais sont placés au-dessus d'un transport UDP/TCP.

Le principe du protocole RTP (Real-time Transfert Protocol) est de fournir un moyen uniforme de transmettre sur IP des données soumises à des contraintes de temps réel (audio, vidéo, etc.). Pour ce faire RTP identifie le type de l'information transportée. Il met en oeuvre des numéros de séquence de paquets IP pour reconstituer les informations même si le réseau sous-jacent change l'ordre des paquets. L'information est donc réorganisée afin d'être présentée de manière cohérente chez l'utilisateur.

Par ailleurs, RTP peut être transporteé dans des paquets multicast afin d'acheminer des conversations vers des destinataires multiples.

Le protocole RTCP (Real-time Transfert Control Protocol) est un protocole associé à RTP. Il est basé sur des transmissions périodiques de paquets de contrôle par tous les participants dans la session. Il contrôle les flux RTP et permet de véhiculer des informations basiques sur les participants d'une session, et sur la qualité de service. RTCP mesure les performances mais n'offre pas de garantie de service. Pour cela il faut, employer un protocole de réservation du type RSVP (voir paragraphes consacré à ce sujet).

# 11 - Supports matériels

## 11.1 - Les supports d'archivage

| | |
|---|---|
| **Objectif** | Etat des lieux des technologies et des supports utilisés pour l'archivage électronique |
| **Domaine d'interopérabilité** | Tous les services d'administration électronique |
| **Responsable** | Gabriel Ramanantsoavina |

### 11.1.1 - Description

Aujourd'hui, un grand nombre de types de supports est disponible pour l'archivage. On distingue généralement deux grandes familles : les supports magnétiques et les supports optiques. S'agissant des supports magnétiques nous distinguerons les bandes magnétiques, des disques magnétiques et des nouvelles technologies qui en sont issues. En ce qui concerne les supports optiques nous citerons successivement les CD, puis les DVD et enfin les disques magnéto-optiques.

### 11.1.2 - Normes et standards

| | |
|---|---|
| RIT0087 | Il est RECOMMANDÉ de choisir pour l'archivage électronique des supports de type WORM physique ou logique (Write Once, Read Many), non effaçables, non réinscriptibles et non modifiables. |

Il est donné ci-après une définition élargie du WORM, extraite du projet de norme ISO 18509, évolution de la norme NF Z42-013. Le WORM fait ainsi référence à une méthode d'enregistrement dont la propriété intrinsèque est d'être non effaçable, non réinscriptible et non modifiable.

Trois types particuliers ont été définis :

- Type A : transformation permanente du support, principe des disques optiques avec modification du substrat ;
- Type B : utilisation d'un micro-code WORM inclue dans le support au moment de sa fabrication, reconnu par le lecteur ou le contrôleur et protégé de l'effacement et de la ré-écriture dans des conditions normales d'utilisation, principe des disques magnéto-optiques ou des bandes équivalentes ;
- Type C : génération d'un micro code enregistré avec l'information et destiné à traiter cet enregistrement comme un enregistrement de type WORM par le logiciel de gestion du support, le protégeant du même coup de l'effacement et de la ré-écriture dans des conditions normales d'utilisation, principe des disques magnétiques. Dans certains cas la protection de type WORM peut être limitée à une durée de conservation associée aux données à protéger.

## 11.1.3 - Supports magnétiques

### 11.1.3.1. Les bandes magnétiques

Loin d'être obsolètes, les bandes magnétiques sont encore utilisées comme supports d'archivage alors que les temps d'accès sont plutôt médiocres comparés aux autres supports de stockage optiques ou magnétiques et que leur pérennité est largement contestée. Ceci certainement en raison de leurs coûts très attractifs. Les évolutions technologiques ont cependant été nombreuses dans ce domaine puisque de 1995 à 2003, 19 nouvelles technologies de bandes correspondant à de nouveaux formats ont été mises sur le marché. Durant la seule année 1998, six nouveaux formats ont fait leur apparition. Enfin l'avènement de la notion de WORM logique (« write once, read many ».) a largement contribué à leur utilisation dans les processus d'archivage.
Il est donné ci-après les formats les plus connus et utilisés de nos jours.

**Synthèse des différents formats de bandes magnétiques**

| Format | Fonction WORM | Capacité Go | Débit Mo/s |
|---|---|---|---|
| SLR (Scalable Linear Recording) | | **2 à 70** | 380 Ko/s à 6 Mo/s |
| ADR (Advanced Digital Recording) | | **15 à 60** | 2 à 2,5 |
| DDS (Digital Data Storage) | | **2 à 36** | 0,5 à 3 |
| DLT (Digital Linear Tape) | X | **40 à 80** | 3 à 8 |
| S-DLT (Super Data Linear Tape) | X | **110 à 300** | 11 à 36 |
| LTO (Linear Tape-Open) | X | **100 à 400** | 15 à 80 |
| AIT (Advanced Intelligent Tape) | X | **35 à 100** | 12 |
| S-AIT (Advanced Intelligent Tape) | X | **500** | 30 |
| Bandes ½ pouce | X | **20 à 200** | 10 à 30 |
| Cartouche 3592 | X | **300** | 40 |

Il faut bien garder en mémoire que la capacité de stockage des lecteurs de bandes magnétiques comporte deux données distinctes : la capacité sans compression dite en mode natif et la capacité avec compression matérielle intégrée, en général le double de la précédente.

### 11.1.3.2. Le disque dur magnétique

Quoique le concept ne soit pas nouveau, l'utilisation du disque magnétique comme support d'archivage repose sur la réunion d'au moins trois éléments importants en plus de leur évolution au niveau de WORM logique. Tout d'abord un aspect économique bien sûr avec l'arrivée de l'interface SATA (Serial Advanced Technology Attachment), évolution de la norme ATA (8.3 Mo/s) utilisée pour l'accès aux disques durs et offrant désormais un débit de 150 Mo/s avec une connectique simplifiée ayant pour conséquence de réduire de manière drastique le coût du gigaoctet de stockage sur les disques durs. Ensuite le fait que pour bon nombre d'organisations, les volumes d'informations augmentent sans cesse et que les temps d'archivage s'allongent en conséquence impose l'utilisation de supports de plus en plus rapides. Enfin, le troisième élément est directement lié au mécontentement des utilisateurs qui reprochent fréquemment à leurs équipements leur manque de rapidité et de fiabilité essentiellement lorsqu'il s'agit d'effectuer des interrogations et des restitutions.

Les nouvelles technologies « Disque Dur »

Par rapport à ce que l'on pourrait qualifier de « *phénomène disque dur* » résultant de l'effet conjugué des différents éléments suivants : moins cher, toujours plus de capacité, accès rapide, nouvelle fonction WORM logique ; différents constructeurs se sont orientés vers ce type de support afin de proposer des solutions innovantes pouvant répondre aux besoins d'archivage. On voit aujourd'hui apparaître sur le marché de nouvelles technologies combinant un ensemble d'éléments permettant d'assurer une conservation fiable et pérenne de l'information sur du disque magnétique.

## 11.1.4 - Les supports optiques

Les CD (Compact Disc) et les DVD (Digital Versatile Disc) sont les deux principaux formats optiques. Conçues à l'origine pour constituer un support audio de haute qualité, les spécifications du CD ont ensuite évoluées afin de permettre le stockage des données numériques.

La grande différence du support optique par rapport aux supports magnétiques réside dans sa fiabilité et surtout dans sa pérennité, bien plus élevée car non soumise à des phénomènes physiques naturels dus entre autre au seul caractère magnétique par exemple de la bande qui peut à long terme provoquer un phénomène de « *collage* ». Même si certains constructeurs de disques optiques n'hésitent pas à annoncer des durées de garanties très longues pour leurs supports il y a lieu de modérer une telle information du seul fait qu'au bout de toutes ces années il y a fort à parier que les lecteurs n'existeront plus dans ce format et qu'en conséquence on se retrouvera avec un disque que l'on sera incapable de relire.

Par ailleurs, l'information est stockée d'une façon permanente par modification du substrat, d'où l'origine de la notion de WORM (Write Once Read Many) physique. C'est pourquoi, les supports optiques ont encore tendance à être largement privilégiés lorsqu'il s'agit d'archivage. L'inconvénient majeur étant, cette fois, son prix par rapport à celui de la bande magnétique. La solution pourrait bien venir des nouvelles technologies basées sur le disque magnétique telles que présentées ci-après.

**Récapitulatif des formats amovibles optiques**

| Format | Capacité Go | Débit Mo/s |
|---|---|---|
| CD-ROM | **650 Mo** | 7 (48X) |
| CD-R | **650-700 Mo** | 6,9 |
| CD-RW | **650 Mo** | 1.000 réécritures |
| DVD-ROM / VIDEO | | |
| Simple face | **4,7** | 21 (16X) |
| Simple face double couche | **8,5** | |
| Double face simple couche | **9,4** | |
| Double face double couche | **17** | |
| DVD-R+R | **4,7** | 1,4 |
| DVD-RW+RW | **4,7** | 1.000 réécritures |
| DVD-RAM | **2,6 à 17** | 100.000 réécritures |

## 11.1.5 - La technologie magnéto-optique (MO)

Ni optique, ni magnétique mais les deux à la fois, le magnéto-optique ou MO (magnéto-optical), déjà mentionné précédemment pour les DVD-RAM, va terminer ce descriptif des supports optiques. Cette technologie offre en fait des disques avec des densités très élevées et présente un potentiel encore plus important de progrès à ce niveau, d'où son emploi en matière d'archivage.

**Récapitulatif des formats magnéto optiques**

| Format | Capacité Go | Débit Mo/s |
|---|---|---|
| MO 3,5" | **de 128 à 640 Mo** | 5 |
| MO 5,25" | **de 640 Mo à 2,3 Go** | 5 |
| MO UDO 5,25" 30 | **30** | 8 |
| MO UDO 5,25" 60 (2005) | **60** | 12 |
| MO UDO 5,25" 120 (2007) | **120** | 18 |

## 11.1.6 - Les Juke Box

Afin d'augmenter les capacités directement adressables en ligne mais surtout afin de simplifier les manipulations, signalons que tant pour les bandes que pour les disques optiques existe, ce que l'on a coutume d'appeler, des librairies (ou juke box) lesquelles peuvent contenir une multitude de cartouches ou de disques optiques, accessibles via des systèmes robotisés, autorisant ainsi des capacités de stockage extrêmement importantes pouvant atteindre le téraoctet (To) voire le pétaoctet (Po).

## 11.1.7 - Avantages et inconvénients des technologies présentées selon différents critères

Par rapport à cette grande diversité de supports tant magnétiques qu'optiques, il est clair que les critères de choix devront se porter essentiellement sur la capacité des supports, leur fiabilité par rapport aux différents mécanismes d'enregistrement et bien sûr leur coût. Le critère du taux de transfert (assimilable à la vitesse d'écriture sur le média) est quelque peu marginal dans la mesure où en règle générale les procédures d'archivage sont effectuées à des périodes non critiques.

Comme autres critères, il ne faudra pas oublié l'évolutivité (problème des compatibilités ascendantes), les possibilités de migrations, la sécurité offerte.

## 11.1.8 - Principes de mise en œuvre

Même si dans l'absolu le support idéal existait, ce qui est loin d'être le cas, encore ne faudrait-il pas oublier de prendre en considération les aspects économiques de façon globale. En effet sur ce dernier point il est nécessaire de raisonner non pas sur l'achat ponctuel de tel ou tel support ou technologie mais sur une exploitation simulée de plusieurs années afin de prendre en compte l'ensemble des paramètres : administration, maintenance, remplacement, … Quoiqu'il en soit, le type de support sera avant tout choisi en fonction de critères précis comme la durée de conservation, la criticité des données à conserver, l'accessibilité, la volumétrie et le coût.

Nous pouvons également ajouter comme exigences vis-à-vis des supports qu'ils aient les qualités suivantes :

- Stabilité intrinsèque du support et robustesse ;
- Large diffusion de la technologie et offre multi-constructeurs ou reposant sur des normes publiques ;
- Existence d'outils de contrôle des supports ;
- Chemin d'accès aux données protégé ;
- Simplicité des opérations de recopie ;
- Protection contre l'effacement accidentel.

## 11.1.9 - Composants

*Il n'existe pas encore d'élément référencé.*

## 11.1.10 - Exemples d'initiatives sectorielles

*Il n'existe pas encore d'élément référencé.*

## 11.2 - Les cartes

### 11.2.1 - Description

| | |
|---|---|
| **Objectif** | Ces règles s'adressent aux architectes et chefs de projet responsables de la mise en place d'échanges entre administrations. Elles décrivent plus particulièrement les conditions liées au paramétrage des cartes à puces émises par les autorités administratives et confiées aux usagers et aux agents. Ces cartes sont utilisées comme éléments de sécurisation des accès aux Systèmes d'Information. |
| **Domaine d'interopérabilité** | Tous les services d'administration électronique |
| **Responsable** | Martine Schiavo |

### 11.2.2 - Normes et standards

| | |
|---|---|
| RIT0088 | Il est OBLIGATOIRE que les cartes des usagers, émises par les autorités administratives et qui sont porteuses de bi-clés et de certificats, respectent les spécifications du socle commun cartes IAS version 1.0.1 plus erratum. |
| RIT0089 | Il est OBLIGATOIRE que les cartes des agents, émises par les autorités administratives et qui sont porteuses de bi-clés et de certificats, respectent les spécifications du socle commun cartes IAS version 1.0.1 plus erratum. |

| | |
|---|---|
| RIT0094 | Il est OBLIGATOIRE que les cartes émises par des autorités administratives, et basées sur le socle commun cartes IAS version 1.0.1 plus erratum, soient référencées selon le programme LAB PRG 0x et soient ainsi interopérables avec le middleware (pilote carte) IAS sur les versions de systèmes d'exploitation et avec la liste des messageries et des navigateurs diffusés ainsi qu'avec les lecteurs référencés. |

### 11.2.3 - Principes de mise en œuvre

*Il n'existe pas encore d'élément référencé.*

### 11.2.4 - Composants

*Il n'existe pas encore d'élément référencé.*

### 11.2.5 - Exemples d'initiatives sectorielles

*Il n'existe pas encore d'élément référencé.*

# 12 - Normes et recommandations

## 12.1.1 - La norme en général

Dans un but d'organisation, l'être humain a tendance à édicter des normes précisant ce qui est normal de faire et ce qui ne l'est pas. Les normes varient donc fortement avec les époques, les individus et de manières plus générales avec les modèles de société.

## 12.1.2 - La norme dans le système juridique

Les normes dans le système juridique sont les lois et les codes.

Décret 84-74 du 26 janvier 1984 (JORF du 1er février 1984) fixant le statut de la normalisation, modifié

Selon le décret 84-74,
*« La normalisation a pour objet de fournir des documents de référence comportant des solutions à des problèmes techniques et commerciaux concernant les produits, biens et services qui se posent de façon répétée dans des relations entre partenaires économiques, scientifiques, techniques et sociaux. »*

## 12.1.3 - La norme pour les Systèmes d'Information

Les normes permettent une interopérabilité des systèmes d'information entre eux. Elles sont donc devenues indispensables dans le cadre de la généralisation des échanges au niveau planétaire. Elles doivent ainsi permettent de remplacer aisément un produit par un équivalent quand on rencontre une difficulté quelconque.

Pour essayer de fédérer l'industrie, des organismes publics ou privés réfléchissent et proposent des référentiels appelés normes ou recommandations. Ces organismes publics ou privés sont généralement à but non lucratif, fondés et soutenus par un syndicat d'industriels concernés par le sujet ou par un consortium.

Une norme est un document de référence publié par un organisme de normalisation officiel par exemple l'AFNOR ou l'ISO. Les organismes de normalisation officiels sont des organismes reconnus au niveau national par leurs états (voir chapitre suivant).

Dans le monde anglo-saxon, le vocabulaire ne dispose que d'un seul terme, « *standard* », pour désigner une norme (le terme « norme » est la traduction de « *standard* »). Pour préciser les choses, on parle pour les normes officielles de « ***standards de jure*** ». Un standard est un référentiel publié par une entité privée. Toutefois, on ne parle de standard qu'à partir du moment où le référentiel est très largement diffusé. On parle alors de « ***standard de facto*** ». En informatique les formats HTML ou le format de fichier Microsoft Word sont des exemples très connus.

Le contenu d'une norme peut être protégé par des droits de propriété intellectuelle en plus de ceux de l'éditeur de la norme (par exemple les brevets sur la norme MP3). Pour les normes, dans un tel cas, le propriétaire des droits s'engage à vendre ses droits à tout le monde à un tarif raisonnable et non discriminatoire (vocabulaire employé dans les normes AFNOR et ISO), Par exemple, les spécifications autour des disques compacts (CD) dont les brevets initiaux étaient la propriété de Philips et Sony, ont donné lieu à publications de normes.

Dans le cas général, un fabriquant ou un prestataire de service n'est pas obligé de suivre une norme. Dans certains cas, les règlements (décrets en France, directives dans l'Union européenne) peuvent imposer l'utilisation d'une norme.

### 12.1.4 - L’Elaboration d’une norme

L'élaboration d'une norme ISO est donnée à titre d’exemple. Elle respecte les principes décrits à l’adresse suivante :

http://www.iso.org/iso/fr/stdsdevelopment/whowhenhow/how.html

Les stades successifs menant à la publication d’une norme ISO sont décrits à l’adresse suivante :

http://www.iso.org/iso/fr/stdsdevelopment/whowhenhow/proc/proc.html

### 12.1.5 - La recommandation

Dans les domaines de l’électronique et de l’informatique, le besoin de normalisation des systèmes d’interconnexion et d’échange de données est géré par des organismes qui donnent des recommandations pour une véritable interopérabilité des systèmes.

Les recommandations n’ont pas le statut de normes, car elles ne sont qu’informatives et incitatives. Aucun système de sanction n’est prévu, hormis que la non-reconnaissance d’un système spécifique ou propriétaire le marginalise et le rend inutilisable en pratique.

L'UIT-T s'occupe de la normalisation des transmissions de données sur les liaisons de télécommunications entre autre. Il est le concepteur de recommandations très célèbres comme V.24, X.21 et X.25.

L'EIA (Electronic Industries Association) est un organisme américain créé en 1924, qui normalise le domaine de l’électronique. Il a produit entre autres la célèbre recommandation RS-232 (RS signifie Recommended Standard).

L’OASIS est un consortium qui édicte des recommandations dans les domaines de l’Internet.

# 13 - Les principaux Organismes de normalisation

## 13.1 - Introduction

En Europe communautaire, chaque pays a son institut de normalisation qui fonctionne sous la tutelle de l'État. Ces organismes officiels sont membres d'un comité qui les représente au sein des autorités européennes dont la Commission Européene. Cet organisme est le Comité Européen de Normalisation (CEN) qui est un organisme privé de droit belge qui a son siège à Bruxelles.

La plupart des organismes européens extra-communautaires), le CEN, ainsi que l'ensemble des instituts nationaux, sont membres de l'Organisation internationale de normalisation (ISO).

L'ISO est une organisation non gouvernementale et ses membres ne sont pas, comme dans le système des Nations Unies, des délégations des gouvernements nationaux. L'ISO occupe néanmoins une position privilégiée entre les secteurs public et privé. L'ISO est un organisme privé de droit suisse.

## 13.2 - Organismes officiels

Sont donnés ici, les principaux organismes qui normalisent les domaines afférents aux systèmes d'information au sens large.

### 13.2.1 - Au niveau mondial

Organisation internationale de normalisation (ISO)
Commission électrotechnique internationale (CEI)
Union internationale des télécommunications (UIT).

Ils existent des accords entre ces trois organismes. Par exemple, l'ISO est représenté au sein de l'UIT (avis consultatif). Une répartition des domaines traités est également mise en place.

Dans le domaine du commerce électronique, on peut également citer l'UN/CEFACT (UN Centre for Trade Facilitation and electronic business) qui est le *Bureau central des Nations Unies pour la facilitation du commerce et des échanges électroniques.*

### 13.2.2 - Au niveau européen

Comité européen de normalisation (CEN)
Comité européen de normalisation électrotechnique (CENELEC)
European Telecommunications Standards Institute (ETSI).

### 13.2.3 - Au niveau national

Allemagne : Deutsches Institut für Normung e.V. (DIN).
France : Association Française de Normalisation (AFNOR)
Royaume-Uni : British Standards Institute (BSI)
USA : American National Standards Institute (ANSI)
USA : National Institute of Standards and Technology (NIST)

## 13.3 - Organismes non officiels

Electronic Industries Association (EIA).
European Computer Manufacturers Association (ECMA)
Institute of Electrical and Electronics Engineers (IEEE)
Internet Engineering Task Force (IETF)
Object Management Group (OMG)
Organization for the Advancement of Structured Information Standards (OASIS)
Unicode Consortium (UNICODE)
Web Services Interoperabilty Organisation (WS-I)
World Wide Web Consortium (W3C)

## 13.4 - Difficultés sur les processus de normalisation

Alors qu'une répartition des domaines traités a été mise en place entre les trois grands organismes mondiaux de normalisation (ISO, CEI et UIT) il n'en est pas de même dans les processus de standardisation des services Web. Un climat d'instabilité plane actuellement sur ce domaine.

En particulier, il y a une concurrence entre le W3C (l'organisme de standardisation des technologies du Web) et l'OASIS (consortium d'éditeurs de logiciels).

Dans ce contexte défavorable, les choix technologiques sont particulièrement difficiles à faire, que ce soit au niveau des services Web parfois concurrents, qu'au niveau des versions de certains services.

Par ailleurs, et toujours sur ce même sujet, une nouvelle association est née en février 2002 sous l'impulsion de Microsoft, d'IBM et de BEA Systems. Elle regroupe plus de 130 intervenants. Sa vocation annoncée est de veiller à l'interopérabilité des services Web. Cette organisation est appelée « Web Services Interoperability Organization ». Son site est accessible à l'adresse suivante : http://www.ws-i.org/

Il est à espérer que les travaux collaboratifs de ces différents organes de normalisation (OASIS, W3C et WS-I) finissent par converger vers un modèle normatif stable et unifié.

# 14 - Fiche de lecture

En cas de remarque sur le présent document veuillez remplir la fiche de lecture et l'adresser à l'auteur.

| Identification du document relu |
|---|
| Référence complète du document relu : |
| Auteur (en clair) : |
| Lecteur (s) : Date de renvoi : |

| Remarques générales (fond et forme) |
|---|
| |

| Synthèse des actions à effectuer |
|---|
| |

| Clôture des corrections | | | |
|---|---|---|---|
| Nom | Fonction | Date | Visa |
| | | | |

| N° | Page | Chap. - § | Libellé des remarques et suggestions | Type* | sévérité | Action** |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

type= F = fond; P = forme;

sévérité : M=Majeur , m=mineur

action = R =retenue; NR = non retenue; DT = déjà traitée; ES = en suspens; J=rejetée

# 15 - Gestion du document

| | Nom | Société / Organisation | Date | Signature |
|---|---|---|---|---|
| **Rédigé par** | **Divers auteurs** | | 2005 | |
| | **Pierre MONTIER**<br>**Françoise KAMMOUN** | DGME | 2006 | |
| **Vérifié par** | **Pierre MONTIER**<br>**Françoise KAMMOUN** | DGME | 2006 | |
| **Validé par** | **Pascal SOUHARD** | DGME | 2006 | |

## Statut

| | |
|---|---|
| **Statut du document** | **Appel public à commentaires** |
| **Limitation de diffusion** | *Pas de limitation particulière* |

# 16 - Gestion des versions

| Version | Date | Description | Rédacteur |
|---|---|---|---|
| 0.n | 2005-2006 | Initialisation et rédaction du document. | |
| 0.90 | 07-04-2006 | Révision de l'ensemble du document, diffusion pour remarques via appel public à commentaires. | |
| | | | |
| | | | |
| *0.99* | | *Intégration des remarques et révision générale. Document à présenter au Comité des Référentiels.* | |
| *1.0* | | *Document après publication des Arrêtés ministériels ;* | |
| | | | |
| | | | |
| | | | |