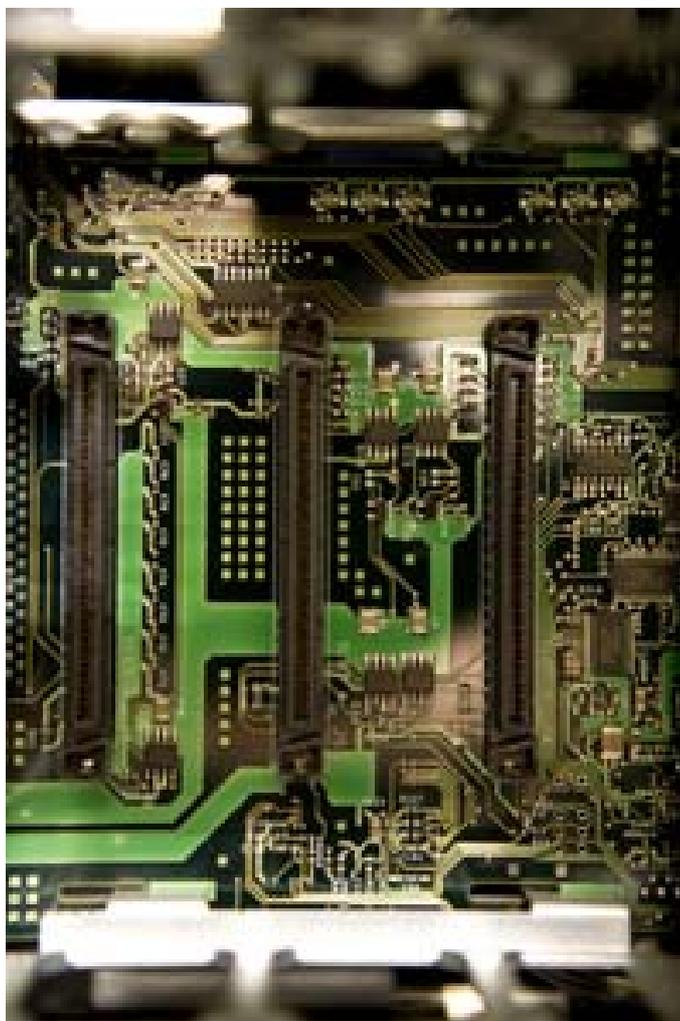


Manuels et guides pratiques

# Exigences types pour la maîtrise de l'archivage électronique

Mise à jour et extension 2008 - Spécifications MoReq2

Texte principal



Direction des Archives de France



# Exigences types pour la maîtrise de l'archivage électronique

Mise à jour et extension 2008 - Spécifications MoReq2  
Traduction française de Marie-Anne Chabin

Titre original : *Model Requirements for the Management of Electronic Records  
Update and Extension 2008 – MoReq2 Specification*



*Ces spécifications ont été préparées  
pour la Commission européenne  
par Serco Consulting et financées  
par le programme IDABC*



Les spécifications MoReq2 sont consultables sous forme électronique sur :

<http://www.DLM-Network.org>

[http://ec.europa.eu/transparency/archival\\_policy](http://ec.europa.eu/transparency/archival_policy)

La présente traduction est disponible en ligne sur le site de la [direction des Archives de France](#). Sa mise en forme, dans la collection électronique des *manuels et guides pratiques* des Archives de France, a été assurée par Pierre Fournié, chef du département des publics. Les liens hypertextes ne sont pas tous actifs dans la première version mise en ligne le 9 décembre 2008 : ils seront activés dans les semaines à venir.

Les traductions en différentes langues devraient prochainement être publiées.

Le texte est également disponible sous forme papier à l'Office des publications officielles des Communautés européennes, en tant que supplément VIII de l'INSAR.

First published in English as

*Model Requirements for the Management of Electronic Records : Update and Extension 2008 –  
MoReq2 Specification*

by the Office for Official Publications of the European Communities

© European Communities, 2008

Reproduction autorisée, sauf à des fins commerciales, moyennant mention de la source.

Mention légale : le copyright de cette publication appartient aux Communautés européennes. La Commission européenne ne garantit pas l'exactitude des informations contenues dans ce document, et décline toute responsabilité de l'utilisation qui pourra en être faite. Les Communautés européennes et/ou leurs institutions ni personne agissant en leur nom ne pourront être tenues responsables d'aucun dommage découlant de l'utilisation de cette publication.

French translation © Direction des Archives de France, 2008

ISBN : 978-2-86000-335-3

En application du Code de la propriété intellectuelle (articles L 122-4 et L 122-5), toute reproduction ou traduction intégrale ou partielle faite sans le consentement de la direction des Archives de France et de l'auteur ou de ses ayants droit ou ayants cause est illicite. Par conséquent, les copies ou les reproductions du présent ouvrage sont strictement réservées à l'usage privé du copiste. Sous réserve que soient indiqués clairement le nom de l'auteur, celui de la direction des Archives de France et la source, la représentation ou la reproduction d'extraits du présent ouvrage à des fins exclusives d'illustration dans le cadre de l'enseignement et de la recherche sont autorisées dès lors que le public auquel cette représentation ou cette reproduction est destinée est composé majoritairement d'élèves, d'étudiants, d'enseignants ou de chercheurs directement concernés et que l'utilisation de cette représentation ou cette reproduction ne donne lieu à aucune exploitation commerciale.

En couverture :

Salle des serveurs du ministère de la Culture et de la Communication

© Direction des Archives de France, photographie François Carlet-Soulages, 2007.

Publié en ligne le 9 décembre 2008 (version 1).

# Sommaire

<i>Textes préliminaires à la version française</i>	7
<b>Préface à la traduction française (projet)</b>	<b>8</b>
<b>Avant-propos de la traductrice</b>	<b>10</b>
<b>0. MoReq2 dans l'environnement français</b>	<b>12</b>
0.1 Le records management aujourd'hui en France	13
0.1.1 Deux textes essentiels depuis 2001	13
0.1.2 Le concept de « records management » dans la culture française	15
0.1.3 La reconnaissance de l'écrit numérique favorise les projets d'archivage électronique	18
0.2 Texte français de MoReq2 : terminologie et principaux concepts	19
0.2.1 Principes de traduction	19
0.2.2 Les concepts essentiels de MoReq2 face aux pratiques françaises	22
0.2.3 Les points forts du SAE selon MoReq2	25
0.3 MoReq2 dans l'environnement normatif	27
0.3.1 Panorama des normes et textes de référence relatifs au « records management »	27
0.3.2 Le records management et la conservation numérique	29
0.3.3 Le records management et les « normes » archivistiques	33
0.4 Tendances et évolutions des projets d'archivage en France	36
0.4.1 Dans le secteur public	36
0.4.2 Dans le secteur privé	42
0.5 Références et bibliographie	45
0.5.1 Code du patrimoine	45
0.5.2 Code civil et autres textes réglementaires relatifs à la signature électronique	46
0.5.3 Autres références réglementaires relatives à la conservation numérique	49
0.5.4 CNIL	50
0.5.5 Référentiel général d'interopérabilité	51
0.5.6 Circulaires de la Direction des Archives de France	52
0.5.7 Guides pratiques	52
0.5.8 Sites Internet	53
 <i>MoReq2 Exigences types pour la maîtrise de l'archivage électronique Mise à jour et extension – 2008</i>	 <b>55</b>
<b>Préface</b>	<b>56</b>
<b>1. Introduction</b>	<b>57</b>
1.2. Historique	57
1.3. Relation entre MoReq et MoReq2	57
1.4. Objectif et champ d'application de ces spécifications	58
1.5. Qu'est-ce qu'un SAE ?	59
1.6. Comment utiliser ces spécifications ?	59
1.6. Propriété intellectuelle	60
1.7. Points forts et limites de ces spécifications	60
1.8. Remarques à destination des États membres	61
1.9. Personnalisation des spécifications	62
1.10. Organisation des spécifications	63
1.11. Tests de conformité	64
1.12. Exigences obligatoires et souhaitables	64
1.13. Commentaires sur les spécifications	65
<b>2. Panorama des exigences d'un SAE</b>	<b>66</b>
2.1 Termes essentiels	66
2.2 Concepts fondamentaux	70
2.3 Modèle des relations entre entités	75
<b>3. plan de classement et organisation des dossiers</b>	<b>78</b>
3.1 Configurer le plan de classement	79
3.2 Séries et dossiers	83

3.3 Volumes et sous-dossiers	86
3.4 Maintenance du plan de classement	89
<b>4. Contrôles et sécurité</b>	<b>95</b>
4.1. Accès	95
4.2. Historique des événements	99
4.3. Sauvegarde et restauration	103
4.4. Documents vitaux	104
<b>5. conservation et destruction</b>	<b>106</b>
5.1 Règles de conservation/destruction	106
5.2 Révision du sort final	113
5.3 Transfert, export et destruction	115
<b>6. Capture et déclaration des documents</b>	<b>120</b>
6.1 Capture	121
6.2 Import par lots	129
6.3 Gestion des messages électroniques	132
6.4 Types de documents archivés	137
6.5 Numérisation et traitement de l'image	137
<b>7. identification</b>	<b>142</b>
7.1 Codes de classement	144
7.2 Identifiants système	147
<b>8. Recherche, repérage et restitution</b>	<b>149</b>
8.1 Recherche et repérage	149
8.2 Restitution : affichage des documents	154
8.3 Restitution : impression	155
8.4 Restitution : autres cas	157
<b>9. Fonctions d'administration</b>	<b>158</b>
9.1 Administration générale	158
9.2 Reporting	159
9.3 Modification, suppression et masquage des documents archivés	164
<b>10. Modules optionnels</b>	<b>168</b>
10.1 Gestion des archives physiques (non électroniques)	169
10.2 Destruction des archives physiques	172
10.3 Gestion électronique de documents et travail collaboratif	173
10.4 Workflow	178
10.5 Gestion de dossiers sériels	183
10.6 Intégration avec les systèmes de gestion de contenu	187
10.7 Signature électronique	190
10.8 Chiffrement	193
10.9 Gestion des droits numériques	194
10.10 Systèmes distribués	197
10.11 Travail hors ligne et à distance	199
10.12 Intégration du fax	201
10.13 Niveaux de sécurité	203
<b>11. Exigences non fonctionnelles</b>	<b>209</b>
11.1 Convivialité	210
11.2 Performance et extensibilité	214
11.3 Disponibilité du système	217
11.4 Normes techniques	217
11.5 Environnement législatif et réglementaire	219
11.6 Externalisation des données et recours à des tiers	219
11.7 Conservation à long terme et obsolescence technologique	221
11.8 Processus métier	225
<b>12. exigences liées aux métadonnées</b>	<b>229</b>
12.1 Principes	229
12.2 Exigences générales	229
<b>13. Modèle de référence</b>	<b>233</b>
13.1 Glossaire	233
13.2 Modèle relationnel des entités	245
13.3 Description des relations entre entités	248
13.4 Modèle de contrôle d'accès	250

<b>Annexes</b>	<b>253</b>
<b>Annexe 1 – Publications de référence</b>	<b>254</b>
<b>Annexe 2 – élaboration de ces Spécifications</b>	<b>255</b>
<b>Annexe 3 – Utilisation de ces Spécifications au format électronique</b>	<b>258</b>
<b>Annexe 4 – Remerciements</b>	<b>260</b>
<b>Annexe 5 – Correspondance avec d’autres Modèles</b>	<b>264</b>
<b>Annexe 6 – traitement des Dates</b>	<b>267</b>
<b>Annexe 7 – Normes et autres recommandations</b>	<b>268</b>
<b>Annexe 8 – Changements par rapport à MoReq</b>	<b>278</b>
<b>Annexe 9 – Modèle de metadonnées</b>	<b>282</b>

# **MoReq2**

## **Exigences types pour la maîtrise de l'archivage électronique**

**Mise à jour et extension – 2008**

---

---

# Préface

## Mise à jour et extension des Exigences types pour la maîtrise de l'archivage électronique

Depuis sa première publication en 2001, le MoReq initial - Modèle d'exigences pour l'organisation de l'archivage électronique - a été largement utilisé dans toute l'Europe et au-delà. Dans toute l'Union européenne, ceux qui ont expérimenté l'archivage électronique ont reconnu l'intérêt d'utiliser un modèle de spécifications tel que MoReq comme base de travail pour l'acquisition d'un système d'archivage électronique et les fournisseurs de logiciels ont, de leur côté, utilisé MoReq dans leur processus de développement.

Le succès de MoReq est aujourd'hui indiscutable. Il a été souvent cité dans de nombreux pays et joue un rôle central dans le monde du records management et de l'archivage électronique.

Ceci dit, les technologies de l'information ont changé depuis 2001. De nombreuses technologies se sont développées avec des changements évolutifs affectant la création, la capture et la gestion des documents archivés électroniquement. Cette nouvelle version de MoReq, appelée MoReq2, prend en compte l'impact de ces changements. Elle tient compte également des nouvelles normes et des bonnes pratiques de ces dernières années. MoReq2 constitue donc une mise à jour évolutive du MoReq initial.

MoReq2 permet, et c'est une première, la mise en œuvre d'une batterie de tests logiciels. Il est précisément rédigé pour faciliter des tests de conformité indépendants : une série de tests de conformité a été développée et est publiée à côté du modèle d'exigences. Le besoin d'exigences explicites et testables a ainsi conduit à plusieurs changements de vocabulaire et de formulation dans MoReq2.

Enfin, ces années d'expérimentation sur la base de MoReq ont mis en évidence le besoin de spécificités nationales concernant les différentes langues, la législation, la réglementation et les pratiques archivistiques traditionnelles. C'est pourquoi MoReq2 a choisi d'inclure un dispositif de pondération - appelé chapitre zéro - pour l'ajout des exigences particulières des États membres.

MoReq2 a été préparé pour la Commission européenne par Serco Consulting et financé par le programme IDABC. Le processus de développement a été supervisé par la Commission européenne en étroite concertation avec le DLM Forum et les principales versions du document ont été relues par les experts du DLM Forum. Ces relectures ont été complétées par celles de dizaines d'utilisateurs, consultants, fournisseurs, institutions et associations professionnelles du monde entier, conférant ainsi à MoReq2 une autorité sans précédent. Ainsi, MoReq2 sera précieux pour tous ceux qui sont intéressés au records management et à l'archivage électronique en Europe et dans le monde.

# 1. Introduction

## 1.1 HISTORIQUE

---

Le besoin de spécifications complètes sur les exigences de l'archivage électronique à des fins de preuve (records management) a été initialement formulé par le DLM-Forum<sup>1</sup> en 1996 comme une de ses dix actions. En conséquence le programme IDA (Echanges de données entre les administrations) de la Commission européenne a passé commande du développement d'un modèle de spécifications pour les systèmes d'archivage électronique (SAE). MoReq - *Modèle d'exigences pour l'organisation de l'archivage électronique* - a été publié en 2001.

MoReq a été largement utilisé dans toute l'Union européenne et au-delà. Cependant il n'existait ni maintenance du modèle ni test de conformité des logiciels aux spécifications MoReq.

Pour répondre à une demande de mise à jour de MoReq et d'un schéma de test de conformité, le DLM Forum a sollicité la Commission européenne. Les discussions ont abouti au lancement en 2006 par le Secrétariat général de la Commission (Directorate B - e-domec et archives) d'un appel d'offre pour le développement de ce document, MoReq2. Le développement a été réalisé au cours de 2007 par une petite équipe de consultants spécialisés de Serco Consulting (ex Cornwell Management Consultants plc), avec l'appui d'un Comité éditorial composé d'experts de plusieurs pays, et de très nombreux relecteurs bénévoles du secteur public comme du privé.

L'annexe 2 donne le détail de la méthodologie suivie, et l'annexe 4 remercie les membres du panel de relecteurs qui ont accepté de donner de leur temps, de leur compétence et de leur expérience.

## 1.2 RELATION ENTRE MOREQ ET MOREQ2

---

MoReq2 vise à remplacer MoReq.

Les spécifications pour MoReq2 figurent dans le rapport détaillé pour le développement de MoReq2. Les buts y sont décrits ainsi :

« Le but de MoReq2 est d'étendre les exigences fonctionnelles des spécifications originales dans un contexte européen et de permettre le développement d'un système de tests de conformité par :

---

<sup>1</sup> DLM est l'acronyme pour « Document Lifecycle Management » (autrefois « Données Lisibles par Machine », en anglais « Machine-readable data »). Le DLM-Forum s'appuie sur les conclusions du Conseil européen (94/C 235/03) du 17 juin 1994 relatives à une plus grande coopération dans le domaine des archives.

- le renforcement des aspects de MoReq qui sont devenus essentiels et l'ajout de nouveaux sujets qui sont importants et qu'il faut clarifier ;
- la testabilité des exigences fonctionnelles avec le développement d'outils de test permettant d'évaluer la conformité des logiciels avec ces exigences ;
- la formulation d'exigences modulaires pour faciliter leur mise en œuvre dans des environnements variés. »

« Dans un souci de compatibilité, MoReq2 est conçu comme une mise à jour évolutive du MoReq initial et non un produit radicalement différent. »

Le concept de « mise à jour évolutive » est essentiel. MoReq2 est complètement compatible avec MoReq (les incompatibilités mineures sont clairement indiquées) ; les concepts et la structure du document sont les mêmes.

## 1.3 OBJECTIF ET CHAMP D'APPLICATION DE CES SPECIFICATIONS

---

Ces spécifications constituent la seconde version des *Exigences types pour la maîtrise de l'archivage électronique* (MoReq2). Elles insistent surtout sur les exigences fonctionnelles pour la maîtrise des documents électroniques à valeur probante par un système d'archivage électronique (SAE).

Ces spécifications s'adressent aussi bien aux organismes publics qu'aux entreprises privées qui veulent se doter d'un SAE ou qui souhaitent évaluer les capacités du SAE dont elles disposent déjà.

Tout en mettant l'accent sur les exigences fonctionnelles, les spécifications soulignent que les critères non fonctionnels jouent un rôle central dans le succès d'un SAE, comme de tout système d'information. Ces critères non fonctionnels sont toutefois tributaires de l'environnement. Ils ne sont donc présentés que dans les grandes lignes.

D'autres exigences connexes, liées notamment à la gestion électronique des documents (GED) et à la gestion des archives physiques (papier ou microfilm) sont également abordées mais dans un moindre détail. Les questions de la numérisation ou autres moyens de création de documents électroniques dépassent le cadre de ces spécifications qui n'abordent pas non plus les aspects pratiques de mise en œuvre d'un SAE.

Ces spécifications partent du principe que les utilisateurs ne se limitent pas aux administrateurs, records managers ou archivistes, mais que les équipes administratives et opérationnelles utilisent aussi quotidiennement le SAE quand elles créent ou reçoivent des documents à archiver ou recherchent des documents archivés.

Ces exigences types se veulent tout à fait génériques. Elles ne prennent en compte aucune plate-forme particulière ni aucune problématique métier spécifique. Grâce à leur modularité, les communautés utilisatrices pourront ajouter les fonctionnalités propres à leur secteur d'activité (voir section 1.6 et annexe 3 pour plus de détails sur l'utilisation et la personnalisation des spécifications).

## 1.4 QU'EST-CE QU'UN SAE ?

---

Un SAE est avant tout une application pour l'archivage des documents électroniques, bien qu'il puisse aussi servir à la gestion des archives papier. Le texte met clairement l'accent sur l'archivage électronique.

La maîtrise de l'archivage électronique est complexe et requiert la mise en œuvre d'un grand nombre de fonctionnalités conformes aux besoins métier. Le système correspondant - un SAE - requiert donc une solution dédiée, même si les systèmes opérationnels et les applications métiers intègrent de plus en plus de fonctionnalités d'archivage. Cette solution dédiée peut être un outil unique, un ensemble d'outils intégrés, un développement spécifique ou une solution mixte. Dans tous les cas, elle devra être confortée par un jeu de politiques et de procédures. La nature d'un SAE varie d'une entreprise ou d'une organisation à l'autre. Ces spécifications ne préjugent pas de la nature des solutions individuelles. Les utilisateurs détermineront comment les fonctionnalités d'un SAE peuvent être mises en œuvre pour répondre à leurs besoins.

Les SAE sont censés être utilisés sur de longues périodes et interagir, de plus en plus, avec d'autres applications. Il y a dès lors plusieurs façons de connecter un SAE avec d'autres applications. Des interfaces peuvent s'avérer nécessaires pour la capture des documents individuels à partir d'autres applications (voir section 6.1) et pour que ces applications puissent accéder aux documents archivés dans le SAE (voir section 4.1). C'est particulièrement vrai pour les applications de type « gestion de la relation client » (CRM) ou d'autres applications métiers.

Le chapitre 10 est consacré aux interfaces avec les outils de gestion de contenu (CMS), les workflows, les systèmes de gestion de dossiers et les fax. Le chapitre 6 traite des interfaces avec les outils de messagerie (section 0.6.3) et la numérisation et le traitement de l'image (section 6.5). L'interface pour la validation des métadonnées est abordée dans la section 6.1 (Capture) et la production de rapports dans la section 8.3 (Impression).

L'objectif initial de MoReq2 est de décrire un logiciel conçu spécifiquement pour l'archivage. Il peut toutefois être également utilisé comme la description des résultats attendus d'un archivage électronique. Dans ce sens, les phrases de MoReq2 du type "Le SAE doit ou devrait..." peuvent être lues comme un raccourci de "Le système utilisateur et/ou le fournisseur de la plate-forme doit ou devrait..." Les lecteurs de MoReq2 décideront quelles exigences correspondent à leur environnement.

La série complète des exigences de MoReq2 est destinée à des systèmes intégrés. Dans certaines situations, un sous-ensemble de ces exigences suffira, par exemple quand les besoins d'archivage sont ceux d'un système de gestion de dossiers ou d'une application métier.

Les modules optionnels 10.4 Workflow et 10.5 Gestion de dossiers visent plus particulièrement les applications métiers. Toutefois, un bon nombre des fonctionnalités énoncées tout au long de MoReq2 pourrait et devrait être pris en considération dans l'implémentation des systèmes métiers.

## 1.5 COMMENT UTILISER CES SPECIFICATIONS ?

---

Les spécifications MoReq2 s'adressent :

- aux utilisateurs potentiels d'un SAE comme base de travail pour préparer un appel d'offre ;
- aux utilisateurs d'un SAE pour l'audit et le contrôle d'un SAE existant ;

- aux organismes de formation comme document de référence pour l'enseignement du records management et de l'archivage et comme support de cours ;
- aux institutions de l'enseignement supérieur comme ressource pédagogique ;
- aux fournisseurs et développeurs de systèmes d'archivage pour guider les développements en soulignant les fonctionnalités exigées ;
- aux prestataires en archivage pour orienter la nature des prestations offertes ;
- aux futurs utilisateurs d'un service d'archivage externalisé comme une aide à la définition des prestations souhaitées.

En outre, pour l'utilisation de la documentation de test développée en parallèle de MoReq2, elles s'adressent :

- aux fournisseurs et développeurs de SAE : pour tester la conformité à MoReq2 des solutions d'archivage électronique ;
- aux utilisateurs de SAE : pour tester la conformité à MoReq2 de la mise en œuvre des SAE.

Les spécifications ont été rédigées en mettant l'accent sur leur utilisation. L'objectif a été de proposer des spécifications faciles à utiliser.

## 1.6 PROPRIETE INTELLECTUELLE

---

Les droits de propriété intellectuelle sur MoReq2, y compris l'utilisation du nom MoReq2, appartiennent à la Commission européenne. En conséquence, toute traduction de MoReq2 ou toute publication d'un chapitre zéro doit être préalablement agréée par la Commission - voir l'avertissement en page de titre. Pour formuler une demande, voir le site du DLM Forum : <http://www.DLM-Network.org>.

## 1.7 POINTS FORTS ET LIMITES DE CES SPECIFICATIONS

---

Les spécifications MoReq2 sont délibérément rédigées dans un esprit pragmatique et utilitaire. L'objectif principal est d'être un outil pratique pour aider les entreprises/organisations à répondre à leurs besoins en matière d'archivage tant électronique que papier. Ces spécifications s'appuient à la fois sur l'archivistique traditionnelle et sur le *records management* mais ces disciplines ont été transposées à l'environnement électronique. Ainsi, MoReq a été élaboré en pensant aussi bien aux besoins des responsables de l'archivage électronique que de l'archivage papier.

La mise en œuvre des exigences de MoReq2 devrait conduire à un système en mesure d'archiver les documents électroniques avec les niveaux de confidentialité et d'intégrité voulus, en combinant les avantages de la gestion électronique à ceux de la théorie classique du *records management*. Cette approche pragmatique inclut par exemple l'introduction d'exigences pour la GED, le workflow, les métadonnées ou d'autres technologies proches.

Bien que MoReq2 couvre un large éventail de types de documents archivables, il faut souligner que les solutions SAE visent souvent les documents dits communément « non structurés »<sup>1</sup>. Pour simplifier, les documents non structurés contiennent des informations dans une forme destinée avant tout à des utilisateurs humains. Ces documents sont par exemple : des lettres, des notes, des messages électroniques, des images, des photocopies, des images scannées, des enregistrements audio et vidéo. A l'inverse, les documents structurés contiennent des informations organisées avant tout pour une utilisation par des applications informatiques (par exemple, les enregistrements d'un système comptable ou d'un système de planification de la fabrication ou encore d'un système de contrôle du trafic aérien). Bien qu'un SAE puisse en principe être utilisé pour archiver et conserver des documents structurés, c'est assez rare. Le plus souvent, les données structurées sont stockées et gérées dans un système de gestion de données métier (application de comptabilité, une application de planification de la fabrication ou une application de contrôle du trafic aérien, etc.). Les solutions SAE sont presque toujours utilisées pour conserver et gérer des documents non structurés. Les cas d'utilisation pour des documents structurés sont généralement liés à un environnement de gestion de dossiers - voir la section 10.5.

MoReq2 ne couvre pas les autres aspects pratiques de l'archivage. Ces spécifications se limitent délibérément aux fonctionnalités requises pour un logiciel d'archivage électronique. Elles ignorent les considérations philosophiques sur le *records management*, l'archivistique théorique, le management, le contrôle de gestion, etc., ces sujets étant largement traités par la littérature existante dont on trouvera une liste à l'annexe 1. A titre d'exemple, les spécifications précisent à plusieurs reprises que certaines fonctions doivent être réservées aux administrateurs. Ceci ne signifie pas que les administrateurs ont à décider de la politique d'archivage mais simplement qu'ils doivent être les seuls utilisateurs missionnés par la direction pour la mettre en œuvre au travers du SAE.

Il est important de noter que la politique d'archivage doit être intégrée aux exigences techniques et métiers de l'entreprise/organisation et que seul un administrateur peut mettre en œuvre, d'un point de vue archivage et d'un point de vue système, les décisions prises par la direction générale.

Enfin, ces spécifications sont délibérément centrées sur les utilisateurs et utilisent le plus possible le vocabulaire des usagers des documents électroniques. Par exemple, le texte décrit les dossiers électroniques comme « contenant » des documents, pour une meilleure compréhension, bien que ces dossiers à proprement parler ne contiennent rien. Voir les détails à la section 2.2.

## 1.8 REMARQUES A DESTINATION DES ÉTATS MEMBRES

---

Comme il a été dit ci-dessus (cf. section 1.3), ces spécifications s'efforcent de prendre en compte un large panel d'exigences - pour différents pays, différents secteurs d'activité et différents types de documents archivables. Ce cadre très large est délibéré mais présente corollairement des limites ; en effet, ce seul document ne peut correspondre à toutes les exigences possibles sans être amendé. Chaque pays a ses traditions, ses points de vue et son environnement réglementaire pour la maîtrise de l'archivage. Ces éléments devront être pris en compte dans l'application de ce modèle d'exigences, particulièrement dans la

---

<sup>1</sup> On peut considérer que tous les documents électroniques correctement archivés sont structurés dans la mesure où ils sont reliés à des métadonnées, à un historique, etc. de manière structurée. Il serait donc plus exact de parler de « documents au contenu non structuré » ; mais cette formulation étant peu répandue, MoReq2 ne l'a pas retenue.

définition d'un nouveau système. C'est pourquoi MoReq2 a prévu que chaque pays de l'Union européenne puisse ajouter un "chapitre national" ou "chapitre zéro" pour exposer les exigences nationales, à savoir :

- traduction des termes essentiels et des concepts clés ;
- exigences des lois et de la réglementation nationales ;
- normes et recommandations sur l'accès à l'information ;
- autres exigences nationales (le cas échéant) ;
- sources d'information complémentaires.

## 1.9 PERSONNALISATION DES SPECIFICATIONS

---

Les exigences de ces spécifications sont seulement destinées à servir de modèle. Elles ne sont pas prescriptives pour toutes les mises en œuvre de SAE ; certaines exigences ne conviennent pas à certains environnements. Par ailleurs, le secteur d'activité, la taille du projet, le type d'organisation et d'autres facteurs suggéreront l'ajout d'exigences spécifiques.

C'est pourquoi, l'utilisation de ces spécifications pour un cahier des charges de solution exige d'abord une personnalisation sur les points suivants :

- ajout ou retrait d'exigences selon les besoins spécifiques de l'entreprise/organisation ;
- ajustements ou précisions, par exemple :
- exigences demandant plusieurs résultats possibles modifiées pour ne demander qu'un seul résultat ;
  - exigences en termes de volumes et de performance.
- introduction d'éléments propres à l'organisation, tels que l'environnement technique ;
- préciser si les exigences sont :
  - inchangées par rapport à MoReq2,
  - nouvelles,
  - supprimées,
  - adaptées.

Ces spécifications ont été élaborées pour être utilisées sous forme papier ou électronique. Elles ont été rédigées à l'aide de Microsoft Word 2003, et publiées dans les formats suivants :

- Microsoft Word 97-2003 (Version 11);
- Microsoft Word 2007 (Version 12);
- Adobe PDF (Version 1.4).

L'utilisation de la forme électronique présente de nombreux avantages. Voir le détail en annexe 3.

## 1.10 ORGANISATION DES SPECIFICATIONS

Les spécifications sont organisées en chapitres divisés en sections.

Le chapitre suivant (chapitre 2) présente un panorama des principales exigences, en commençant par la terminologie, fondamentale dans ces spécifications.

Les chapitres 3 à 9 exposent le détail des exigences fonctionnelles d'un SAE. Chaque chapitre contient un ensemble logique d'exigences fonctionnelles. Certains recouvrements entre les chapitres sont toutefois inévitables, en raison même du sujet.

Le chapitre 10 comporte plusieurs sections, présentant les exigences pour différents modules optionnels d'un SAE. Certaines sections (par exemple sur les systèmes distribués) seront essentielles pour telle ou telle entreprise/organisation mais sans objet pour d'autres.

Le chapitre 11 traite des exigences non fonctionnelles.

Le chapitre 12 énonce les exigences relatives à la gestion des métadonnées ; le détail des métadonnées nécessaires à MoReq2 figurent dans l'annexe 9.

Le chapitre 13 comporte un modèle de référence de SAE tel qu'il est compris dans ces spécifications. Ce modèle peut être utilisé pour comprendre les aspects clés des spécifications, notamment les définitions des termes utilisés (série, sous-dossier, volume) et leurs relations (exemple : « que peut-on stocker dans un dossier électronique ? »).

Les annexes donnent la liste des documents de référence, des indications d'ordre administratif ou autre. L'annexe 9 présente le modèle de métadonnées de MoReq2. Il figure à part du reste de MoReq2 pour faciliter son utilisation et en raison de sa longueur.

Pour répondre à diverses demandes, des outils de test ont été développés pour compléter ces exigences. Les outils de test sont publiés sous forme électronique en parallèle des exigences. La structure de MoReq2 est conçue pour faciliter les tests de conformité aux exigences ; chaque section du chapitre 10 constitue un module de test optionnel. Pour plus de détail sur ces tests, voir <http://www.DLM-Network.org>.

Les exigences sont présentées sous forme de tableau, à raison d'une exigence par ligne, comme indiqué dans la figure 1.1.

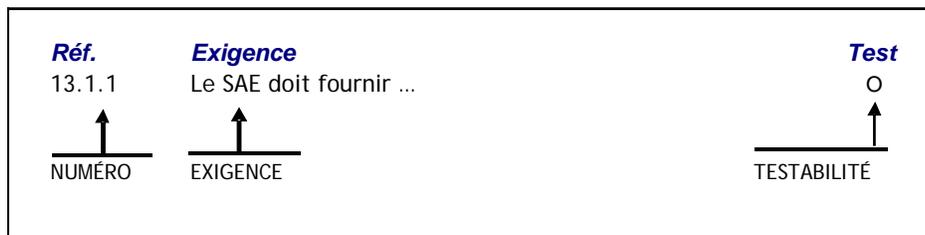


Figure 1.1

Chacune des exigences est numérotée et formulée en langage courant.

## 1.11 TESTS DE CONFORMITE

---

### Testabilité

Chaque exigence est assortie d'un attribut de test qui indique s'il est possible de tester la conformité à cette exigence. Les valeurs possibles de ces attributs de testabilité sont les suivants :

- **O** - L'exigence peut être testée. Exemple : *"Le SAE doit permettre au moins trois niveaux hiérarchiques dans le plan de classement"*. Le test consiste à créer une arborescence à trois niveaux.
- **N** - L'exigence ne peut pas être testée. Exemple : *"Le SAE doit supporter le plan de classement métier de l'entreprise/organisation"*. Cette fonction n'est pas testable dans l'absolu.
- **P** - L'exigence peut être testée mais le test sera partiel, et/ou la conformité peut s'avérer lacunaire. Exemple : *"Le SAE ne devrait pas limiter le nombre de niveaux hiérarchiques"*. Il n'y a pas réellement moyen de tester une absence de limite. Toutefois, l'exigence est partiellement testable : si on crée un assez grand nombre de niveaux, le test permet alors de remarquer si le nombre de niveaux est limité ou non ; s'il l'est, le SAE ne sera pas conforme à l'exigence.

### Au-delà du SAE

Ces spécifications sont assorties d'un cadre de test de MoReq2. Ce cadre fournit un guide qui documente les tests de conformité d'un SAE à MoReq2.

Plusieurs exigences de MoReq2 sont relatives aux matériels et logiciels, ce qui dépasse le cadre du SAE *stricto sensu*. MoReq2 comporte par exemple :

- des exigences relatives à l'intégration des courriels, liée au logiciel de messagerie ;
- des exigences d'évolutivité et d'intégrité, liées à l'outil de gestion de bases de données ;
- des exigences relatives à la numérisation, liées à l'outil de scan.

Il est bien évidemment impossible de tester un SAE avec tous les matériels et logiciels potentiellement utilisables. On part donc du principe que ces exigences seront testées avec un dispositif matériel-logiciel spécifié par le fournisseur du SAE. Le certificat de conformité précisera quel matériel et quel logiciel ont servi aux tests, la conformité se limitant à cet environnement. Les utilisateurs du SAE désireux de connaître la conformité à un autre logiciel ou matériel devront l'évaluer au cas par cas.

## 1.12 EXIGENCES OBLIGATOIRES ET SOUHAITABLES

---

MoReq2 comporte des exigences obligatoires et des exigences souhaitables. La distinction est indiquée comme suit :

- le mot « doit » indique que le caractère obligatoire de l'exigence,
- le mot « devrait » indique que le caractère optionnel de l'exigence.

Dans tous les cas, le niveau d'exigence dépend du contexte. Par exemple, une exigence obligatoire dans un module optionnel n'est obligatoire que dans le contexte de ce module.

Dans certains cas, le caractère obligatoire dépend de la satisfaction d'une exigence optionnelle. Le contexte est en général assez clair, ainsi dans l'exemple suivant :

- 3.1.17 : Le SAE devrait permettre l'export, total ou partiel, du plan de classement.
- 3.1.18 : Si SAE permet l'export, total ou partiel, du plan de classement (cf. 3.1.17), l'export doit inclure les métadonnées [...]

signifie que la fonctionnalité demandée par 3.1.18 est obligatoire si et seulement si la fonctionnalité demandée par 3.1.17 existe.

## **1.13 COMMENTAIRES SUR LES SPECIFICATIONS**

---

Pour formuler des commentaires et des observations, voir les modalités sur le site du DLM Forum : <http://www.DLM-Network.org>

## 2. Panorama des exigences d'un SAE

Ce chapitre commence par la définition de quelques termes essentiels (section 2.1), suivie d'une explication de quelques concepts fondamentaux (section 2.2) et d'un schéma des relations entre entités qui constitue le modèle de base de ces spécifications (section 2.3).

### 2.1 TERMES ESSENTIELS

---

MoReq2 nécessite de préciser le sens de certains mots. Chaque fois que possible, le sens est le sens courant ou le sens généralement admis parmi les professionnels de l'archivage et du records management. Certains mots sont cependant spécifiques à MoReq2. Tous les termes sont définis dans le glossaire (section 13.1) ; quelques définitions du glossaire, essentielles pour la compréhension de MoReq2, sont reproduites ici, à l'identique, pour qu'on s'y réfère plus facilement.

Dans les définitions qui suivent, les termes *en italique* sont définis dans le glossaire, section 13.1.

#### capturer

(1) Action d'enregistrer ou de sauvegarder une instance particulière d'un objet numérique (source: InterPARES 2 Projet de base de données terminologique).

(2) Sauvegarder une information dans un système informatique.

Note : dans MoReq2, la capture des documents désigne l'ensemble des processus conduisant à l'archivage d'un document dans le SAE, c'est-à-dire : l'enregistrement, le classement, l'ajout de métadonnées et la fixation des contenus du document source. Le mot signifie plus généralement une entrée dans le SAE avec le stockage d'informations complémentaires telles que les métadonnées.

#### classement

Dans l'archivage, identification et ordonnancement systématiques des activités métiers et/ou des *documents à archiver* en catégories selon une structure logique prédéfinie, des méthodes et des règles concrétisées dans un plan de classement.

Source : ISO 15489 (voir annexe 7).

#### composant

Train de bit indépendant qui, seul ou combiné à d'autres, constitue un document (archivable ou non).

Note : le mot n'est pas d'usage courant.

Note : l'expression "train de bit indépendant" équivaut à ce qu'on appelle couramment un "fichier" en informatique<sup>1</sup>. Le concept fondamental est qu'un composant fait partie intégrante du contenu du document archivé, même s'il peut être stocké et géré séparément.

Note : un composant sera par exemple :

- Un document HTML et les images JPEG qui constituent une page web ;
- Un document bureautique, texte et tableau, composé d'un document texte avec un lien embarqué (hyperlien) vers un tableur ;

Note : les composants doivent être distincts et séparés les uns des autres. Si un document texte contient un tableau incorporé (par opposition à un hyperlien vers le tableur), le tableau ne doit pas être considéré comme un composant ; dans ce cas, le document texte incluant le tableau ne constitue qu'un seul et même document.

Note : un courriel avec ses pièces jointes peut être un seul composant ou plusieurs, ou même plusieurs documents distincts, en fonction du format des données.

- Si le message est stocké dans un format qui inclut le corps du message et les pièces jointes, il n'y a qu'un composant.
- Si les pièces jointes sont stockées séparément du corps du message mais avec un lien, chaque pièce jointe, de même que le corps du message, est un composant.
- Si les pièces jointes sont stockées séparément du corps du message sans y être reliées, chaque pièce jointe ainsi que le message constituent des documents distincts ; les bonnes pratiques suggèrent de relier ces documents manuellement.

## document<sup>2</sup>

Information enregistrée ou objet qui peut être traité comme une unité.

Source: ISO 15489 (voir annexe 7).

Note : un document peut être sur papier, microforme, support magnétique ou autre support numérique. Il peut comporter toute combinaison de texte, données, graphiques, son, images animées, etc. Un document unique peut être constitué d'un ou plusieurs *composants*.

Note : les simples documents présentent plusieurs différences importantes par rapport aux *documents à archiver ou archivés*. MoReq2 désigne par document une information qui n'a pas été capturée dans le système d'archivage, c'est-à-dire classée, enregistrée, figée pour prévenir toute modification. Le seul fait de capturer ne confère pas la qualité de document archivé. À noter cependant qu'un certain nombre de documents capturés sont archivés.

## document à archiver ou archivé

Documents créés, reçus ou préservés à titre de preuve et d'information par une personne physique ou morale dans l'exercice de ses obligations légales ou la conduite de son activité.

---

<sup>1</sup> Note du traducteur : le mot anglais pour fichier étant "file", il a été évité dans la version anglaise pour éviter la confusion avec le mot dossier ("file" également).

<sup>2</sup> Note du traducteur : dans la traduction française, le mot document désigne parfois les documents archivés, quand le contexte est sans ambiguïté. Par ailleurs, le mot anglais « document » est également rendu par le mot français « pièce » - cas d'un document constitué de plusieurs pièces (record made of several documents).

Source: ISO 15489 (voir annexe 7).

Note : les définitions nationales sont aussi recevables.

Note : un document archivé peut comporter plusieurs pièces (cas des pièces jointes), et peut se présenter sous n'importe quel support et format. Il peut donc être constitué d'un ou plusieurs composants. Outre son contenu informatif, un document archivé devrait inclure une information contextuelle et, le cas échéant, l'information de structure (description des composants, etc.). Une des caractéristiques fondamentales du document archivé est qu'il ne peut plus être modifié.

Note : un SAE peut gérer à la fois l'archivage électronique et l'archivage physique.

#### **document électronique à archiver, document électronique archivé**

Un document à archiver ou archivé sous forme électronique.

Note : la forme électronique peut soit être native (production d'une application informatique), soit résulter d'une opération de numérisation, notamment d'un scan.

#### **dossier**

Ensemble organisé de documents à archiver traitant du même sujet ou procédant de la même activité ou opération.

Source : résumé et adapté de ISAD(G) (voir annexe 7).

#### **dossier sériel**

Un dossier traçant une ou plusieurs opérations effectuées totalement ou partiellement de manière structurée ou semi-structurée, et résultant d'un processus ou d'une action précise.

Note : il n'existe pas de définition universelle de ces termes ni de la distinction entre les dossiers sériels et les autres types de dossiers gérés par un SAE. Il s'agit d'une définition *ad hoc* qui vise à faciliter la compréhension de MoReq2 ; son utilisation dans d'autres environnements n'est pas garantie.

Note : les pièces d'un dossier sériel peuvent être structurées ou non structurées. La caractéristique principale d'un dossier sériel est qu'il résulte d'un processus qui est structuré, au moins en partie, et répétitif. Exemples :

- demandes de permis ;
- réclamations courantes ;
- enquête sur un incident ;
- contrôle régulier.

Note : les autres caractéristiques d'un dossier sériel sont que, en général :

- la structure de leur contenu est prédictible ;
- ils sont produits en nombre ;
- ils sont structurés ou semi-structurés ;
- ils sont gérés par un processus connu et prédéterminé ;
- ils doivent être conservés pendant des durées imposées par la réglementation ;
- ils peuvent être ouverts et clos par des gestionnaires, des utilisateurs finaux ou des systèmes informatiques sans intervention du management.

### métadonnées

(Dans le contexte de l'archivage) Données décrivant le contexte, le contenu et la structure des documents archivés et leur gestion dans le temps.

Source: ISO 15489 (voir annexe 7).

Note : certains modèles reposent sur une conception différente des métadonnées, par exemple en considérant les données d'historiques des événements comme des métadonnées à part entière. Ces approches sont valables dans certains contextes mais ne permettent pas de préciser les fonctionnalités du système et ne sont donc pas retenues ici.

### plan de classement

(dans MoReq2) Organisation hiérarchique des séries, dossiers, sous-dossiers, volumes et documents.

### SAE

Système d'Archivage Électronique

Note : les SAE présentent plusieurs différences importantes par rapport aux systèmes de GED. Voir le détail section 10.3.

### série

(dans MoReq2 seulement) Partie d'un *plan de classement* partant de n'importe quel point de l'arborescence et englobant tous les dossiers en dessous de ce point.

Note : cette définition correspond, en documentation, à une « division primaire », un « groupe » ou une « série » (subdivision, sous-groupe, sous-série, etc.) à n'importe quel niveau du plan de classement.

Note : dans MoReq2, série peut aussi désigner l'ensemble des documents rattachés à une série.

### sous-dossier

Subdivision intellectuelle d'un *dossier*.

Note : les sous-dossiers sont plus spécialement utilisés pour la gestion des dossiers sériels. Dans ce cas, chaque sous-dossier est destiné à conserver un ou plusieurs types de documents entrant dans la composition du dossier, par exemple : "factures", "évaluations", "correspondance". Cette utilisation peut être étendue aux dossiers non sériels.

### volume

Subdivision d'un *sous-dossier*.

Note : ces subdivisions sont créées pour améliorer la maniabilité du contenu des sous-dossiers, grâce à de petites unités faciles à gérer. Elles sont mécaniques (basées sur un nombre de documents, des numéros ou un laps de temps) plutôt qu'intellectuelles.

## 2.2 CONCEPTS FONDAMENTAUX

---

Les concepts fondamentaux pour la bonne compréhension de ces spécifications sont :

- document à archiver et document électronique à archiver ;
- document qui fait autorité ;
- dossier, sous-dossier et volume électronique ;
- plan de classement ;
- série ;
- SAE ;
- capture des documents ;
- profil utilisateur.

### Document à archiver, électronique ou non

Ainsi que l'explique le guide du DLM Forum dans sa section 2.4 (annexe 1), les documents à archiver sont composés :

- d'un contenu ;
- d'une structure ;
- d'un contexte ;
- d'une présentation.

Le contenu réside dans une ou plusieurs pièces, physiques ou électroniques, qui véhiculent le message (l'information) du document à archiver. Elles sont agencées de telle façon que les futurs utilisateurs puissent les appréhender dans leur contexte. Cela suppose qu'un document à archiver comporte, outre les contenus, une information sur sa structure et les métadonnées de contexte et sur sa présentation. Cependant MoReq2 utilise la notion de document à archiver pour désigner l'information principale - le ou les pièces dont le document est constitué - sans inclure les métadonnées. La présentation, quant à elle, découle d'une combinaison des contenus, de la structure et (pour l'électronique) du logiciel de restitution (voir le glossaire).

Dans le monde des archives physiques, la grande majorité des documents forment des dossiers papier, constitués de lots de documents rangés dans des chemises cartonnées. Des contrôles devraient empêcher les utilisateurs de modifier les documents ou leur ordre de classement dans le dossier.

Les mêmes concepts sont valables pour l'électronique. Un document archivable est constitué de plusieurs fichiers électroniques. Ces fichiers peuvent être des documents texte, des courriels, des tableaux, des images fixes ou animées, des fichiers audio ou tout autre objet numérique. Les documents sont dits archivés lorsqu'ils sont sélectionnés et « capturés » dans le SAE. Lors de la capture, ils sont « classés », c'est-à-dire reçoivent le code correspondant à leur série dans le plan de classement, code qui permettra au SAE de les gérer. Les documents sont généralement liés à un dossier - mais pas systématiquement, voir ci-dessous.

Du point de vue de la conservation, il est important de considérer que les documents électroniques possèdent plusieurs composants (composant est utilisé par MoReq2 au sens de fichier). Chaque composant est un objet numérique géré par un système informatique, quel que soit son format ; mais c'est leur assemblage complet qui seul constitue le document archivé. Tous les documents ne sont pas composites ; ainsi, la plupart des documents texte n'ont qu'un composant. Exemple de document à plusieurs

composants : une page web avec du texte, des schémas et des feuilles de style ; il n'est pas rare qu'une page web comporte un composant HTML, des dizaines d'images JPEG, et un jeu de CSS (feuilles de style en cascade).

Une des caractéristiques essentielles du document archivé est que son contenu informationnel est figé. En conséquence, aucune opération visant un document archivé ne doit remettre en cause les relations entre ses composants ; autrement dit, toutes les opérations effectuées sur un document archivé doivent préserver ces relations. Ainsi, en cas de déplacement ou de copie, l'opération doit se faire de telle façon que les composants et leurs interrelations soient maintenus.

### Document qui fait autorité

Pour ISO 15489, un document fait autorité s'il présente les caractéristiques suivantes :

- authenticité ;
- fiabilité ;
- intégrité ;
- exploitabilité.

Comme le précise ISO 15489, le but de tous les systèmes d'archivage devrait être de garantir que les documents qui y sont archivés et stockés font autorité. En résumé, un document fait autorité si :

- il peut prouver qu'il est bien ce qu'il prétend être ;
- il peut prouver qu'il a été créé ou envoyé par la personne qui prétend l'avoir créé ou envoyé ;
- il peut prouver qu'il a été créé ou envoyé à la date prétendue ;
- on peut s'y fier parce que son contenu constitue une représentation intégrale et fidèle des transactions, opérations et faits qu'il décrit ;
- il est complet et non altéré ;
- il peut être localisé, repéré, restitué et interprété.

Les exigences de MoReq2 visent à ce que les documents archivés et stockés dans un SAE conforme à MoReq2 fassent autorité. Toutefois, la satisfaction à ces exigences n'est pas une condition suffisante ; encore faut-il avoir une politique d'entreprise/organisation et s'y conformer.

### Dossier, sous-dossier et volume électronique

Les documents papier sont normalement regroupés en dossiers dans des chemises cartonnées. Les dossiers papier sont rattachés à une structure dite plan de classement. Dans un SAE, les documents électroniques sont gérés dans des dossiers et des répertoires électroniques bien que ceux-ci n'aient pas d'existence réelle ; ils sont virtuels au sens où ces dossiers et répertoires ne « contiennent » rien ; en réalité ce sont les métadonnées attachées aux documents archivés qui créent les dossiers. Il n'est même pas besoin de distinguer dans le système électronique les dossiers et les répertoires. Du reste, ceci est en général transparent pour les utilisateurs du SAE ; le logiciel de SAE leur permet de voir et de gérer des répertoires comme s'ils contenaient physiquement les documents rangés logiquement dans les dossiers. C'est cette approche, centrée sur l'utilisateur, qui est retenue dans ces spécifications : les dossiers électroniques sont définis comme « contenant » des documents par commodité. À noter cependant que si ces spécifications donnent les exigences fonctionnelles pour la gestion des dossiers électroniques, elles ne disent pas comment le concept de dossier électronique est mis en œuvre.

Il peut-être utile de subdiviser les dossiers en sous-dossiers. Cette subdivision est « intellectuelle », dans le sens où c'est en général une personne qui décide dans quel sous-dossier tel document sera classé. Les

sous-dossiers sont fréquemment utilisés dans le cas de dossiers sériels, par exemple des dossiers d'acquisition ou de vente foncière avec des sous-dossiers par opération : publicité, contrat, discussion avec les avocats, etc.

Le sous-dossier représente donc une subdivision du dossier liée au contenu. Il peut donc être utilisé pour attribuer des règles de conservation/destruction différentes à différents groupes de documents au sein du dossier.

Indépendamment de la création de sous-dossiers, les dossiers sont parfois subdivisés « mécaniquement » en volumes, selon des critères prédéfinis. Le terme « mécaniquement » suppose un simple respect de ces critères qui ne sont pas liés au contenu intellectuel des dossiers mais à leur taille, au nombre de documents ou à un laps de temps. Cette pratique, née dans l'environnement papier pour réduire la taille et le poids des dossiers est transposable aux dossiers électroniques pour réduire leur importance matérielle en cas de tri, transfert ou autre. Le concept de volume s'applique particulièrement aux dossiers qui restent ouverts sur de longues périodes et/ou reçoivent de très nombreux documents.

Si la distinction entre les dossiers et les volumes est claire, ses implications peuvent être plus complexes dans la mesure où le choix de créer des volumes se gère différemment selon la nature de l'information et son utilisation :

- certains dossiers sont clos à une date donnée, de sorte que l'unité de gestion est le dossier (même si le dossier est composé de plusieurs volumes), par exemple un petit dossier d'achat, ou le dossier d'un projet.
- certains dossiers ont une durée de vie illimitée (ou quasiment illimitée), de sorte que l'unité de gestion est le volume, par exemple, le dossier d'une circonscription géographique, ou un dossier traitant d'un sujet qui ne se périmé pas, comme la réglementation, ou un dossier de facturation dans lequel un nouveau volume est créé chaque année.

Il peut arriver, rarement, que des documents soient stockés hors dossier et rattachés directement à une série. Voir l'explication au point 3.2.17.

### Plan de classement

L'archivage organise les dossiers de manière structurée et les bonnes pratiques veulent que cette structure reflète les activités de l'entreprise/organisation. Cette structure est appelée « plan de classement ». Le plan de classement est en général hiérarchique. MoReq2 a choisi cette approche hiérarchique, les autres approches sont hors périmètre ; autrement dit une organisation hiérarchique de l'information est un pré-requis pour la conformité à MoReq2.

Les dossiers semblent exister alors s'ils ne sont qu'un groupe de documents ; il en va de même pour les niveaux supérieurs du plan de classement qui semblent exister alors qu'ils ne sont qu'un groupe de dossiers ou de niveaux inférieurs. Comme pour les dossiers, ces spécifications énoncent des exigences de hiérarchie sans être prescriptives sur leur mise en œuvre.

Les dossiers peuvent apparaître à n'importe quel niveau de l'arborescence, comme l'illustre la figure 2.1, qui montre un plan de classement fictif avec ses séries et ses dossiers jusqu'au plus bas niveau. Ce plan de classement fictif est bien sûr plus simple que dans la réalité.

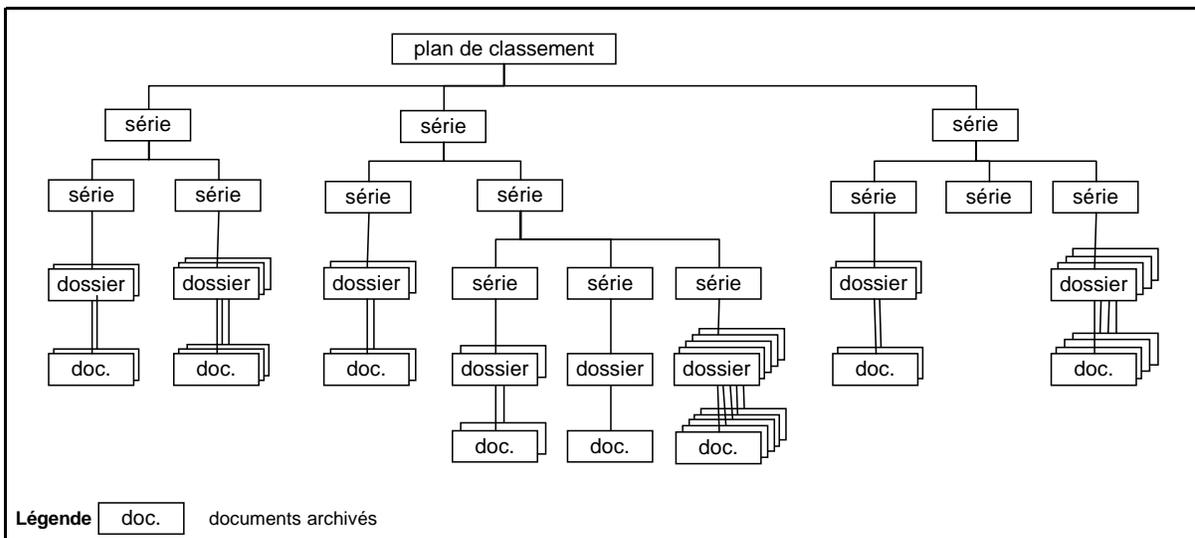


Figure 2.1

A noter que cette figure présente un exemple de relations possibles entre les différents niveaux, dossiers et documents. Elle ne montre pas tous les niveaux ni tous les classements possibles.

### Série

MoReq2 utilise le mot « série » pour désigner la partie d'une arborescence qui part de n'importe quel point et englobe tous les dossiers inférieurs. Le terme série correspond à « groupe » ou « série » (« sous-groupe » ou « sous-série ») dans d'autres textes.

Visuellement, la série d'une arborescence correspond à la branche d'un arbre. Une série peut en inclure d'autres, elles-mêmes subdivisées en sous-séries et sous-sous-séries. Les rectangles ombrés et les traits en gras de la figure 2.2 donnent un exemple de série.

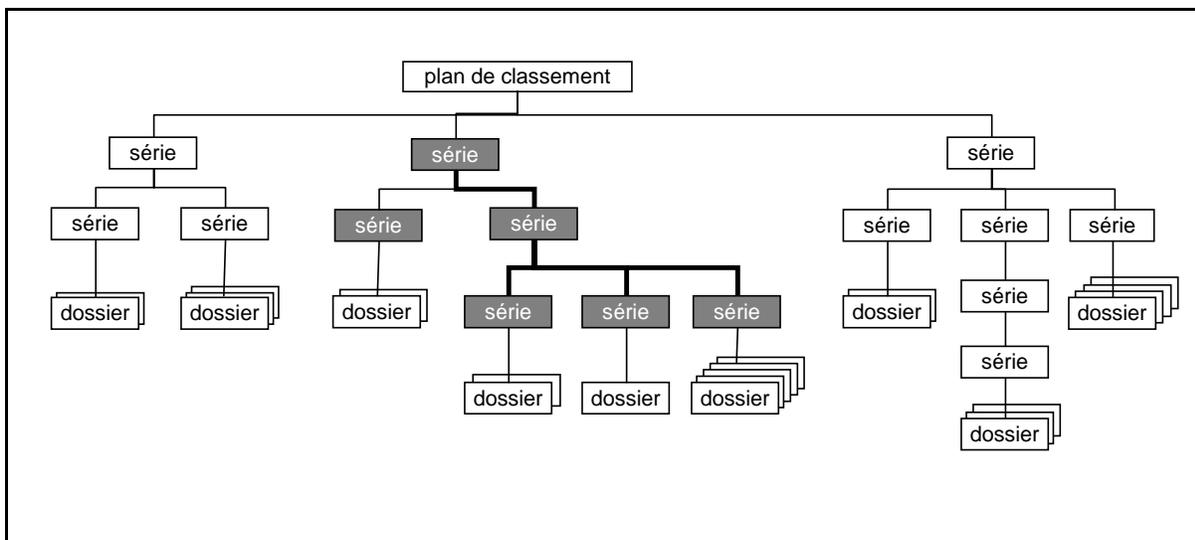


Figure 2.2

MoReq2 utilise également le mot « série » pour désigner l'ensemble des dossiers, documents, etc. rattachés à une série - de même que le mot « bouteille » désigne à la fois le contenant en soi et le contenant avec son contenu liquide. Cette dualité est intentionnelle et le contexte est toujours clair.

MoReq2 utilise les termes « fille » et « mère » pour désigner les relations entre entités. La « fille » d'une entité est l'entité située en dessous dans la hiérarchie (entité descendante). La « mère » est une entité située au dessus dans la hiérarchie. Par exemple, les filles et fils d'une série sont d'autres séries, des dossiers et (rarement) des documents.

MoReq2 permet que des documents soient rattachés directement à une série sans appartenir à un document. Ceci est cependant assez rare et est décrit dans la suite de MoReq2.

### Système d'archivage électronique (SAE)

Un SAE est d'abord une application destinée à l'archivage électronique, bien qu'on l'utilise aussi pour l'archivage physique.

Un SAE est souvent étroitement intégré à un système de gestion électronique de documents (GED) ou une application métier. Techniquement, un SAE gère des documents archivés, tandis qu'un système de GED gère des documents qui ne sont pas ou pas encore archivés. Ceci dit, il est parfois difficile, au quotidien, de séparer leurs fonctionnalités. Ce point est développé dans la section 10.3 qui traite de la GED.

### Capture des documents

Les documents créés ou reçus dans l'exercice des activités sont dits archivés quand ils sont sélectionnés et « capturés » dans le SAE. Lors de la capture, ils sont « classés », c'est-à-dire reçoivent le code correspondant à leur série dans le plan de classement, code qui permettra au SAE de les gérer ; ils reçoivent en outre un identifiant unique.

Très souvent, les documents qui sont sélectionnés, ou capturés, sont archivés dans le cadre d'un processus métier, comme cela se produit dans un workflow. Par exemple, quand une facture est émise, son archivage devrait être déclenché automatiquement. Dans d'autres cas, l'archivage peut être exigé par une procédure métier plus large sans être intégré formellement dans un processus. Ou encore, le processus de capture sera initié par un utilisateur qui choisira les documents à archiver dans le système. Cette sélection des documents à archiver devra s'appuyer sur une analyse de l'environnement réglementaire, des besoins métier, des exigences de responsabilité et du risque à ne pas archiver. Prenons l'exemple des notes dans une entité qui traite de problèmes stratégiques : l'entité peut décider que seules les notes de portée stratégique seront archivées (en général, les notes courantes, concernant l'organisation des réunions, etc. ne seront pas archivées). Il peut arriver que les versions préparatoires aient une portée stratégique ; elles devront alors être archivées en tant que telles ; d'autres fois non. MoReq2 entend répondre à tous ces scénarios. MoReq2 décrit un système à usage général, et non seulement un système d'archivage pour certaines formes d'applications ou pour l'usage exclusif des archivistes ou des administrateurs de systèmes.

### Profils utilisateur et administrateur

MoReq2 utilise le concept d'« utilisateur » pour désigner toute personne dûment autorisée à se servir du SAE. Dès lors, toute personne autorisée à se connecter au SAE est un utilisateur, administrateurs inclus. Toutefois, la distinction entre utilisateur et administrateur peut être complexe ou confuse. C'est pourquoi MoReq2 recourt à la notion de « profils » dans la définition de nombreuses exigences.

Il existe plusieurs façons de mettre en œuvre un SAE. Dans une petite structure, un seul administrateur suffira à gérer la mise en œuvre alors qu'une grande entreprise/organisation aura besoin de plusieurs administrateurs, ayant chacun des autorisations d'accès différentes. Il n'est pas pertinent d'identifier ici tous les accès possibles, d'où la notion de « profils » de MoReq2.

MoReq2 identifie deux profils : les « utilisateurs » et les « administrateurs ». Dans la pratique, on aura au moins une personne de chaque profil, les entreprises/organisations étant libres d'en définir d'autres. Des exemples de profils avec leurs autorisations sont présentés dans une matrice section 13.4.

En résumé, un « profil » dans MoReq2 ressemble à un profil utilisateur - il ne s'agit pas d'un poste ou d'un emploi mais de responsabilités et d'autorisations fonctionnelles partagées par plusieurs utilisateurs. MoReq2 admet deux profils administrateurs et deux profils utilisateurs.

Les profils administrateurs sont chargés de l'organisation des documents archivés ; ils sont concernés par les documents en tant qu'unités de gestion plutôt que par leur contenu métier. Ils gèrent aussi le matériel et logiciel du système, le stockage, les sauvegardes et la performance du SAE.

A l'inverse, les profils utilisateurs ont accès aux fonctionnalités correspondant aux besoins des équipes, y compris l'ajout de documents, la recherche et le repérage des documents archivés ; ils sont intéressés par le contenu des documents plutôt que par leur organisation - autrement dit, ils sont concernés par la valeur métier portée par les documents.

## 2.3 MODELE DES RELATIONS ENTRE ENTITES

---

Cette section comporte avec la figure 2.5 un modèle des relations entre entités qui peut aider à comprendre les spécifications. Pour une explication circonstanciée voir la section 13.3.

A noter que ce schéma ne cherche pas à représenter l'organisation des entités effectivement stockées dans le SAE. Il donne une vue théorique de l'organisation des documents archivés. Un SAE utilise ces relations pour appliquer un traitement similaire à ce qui est proposé par le modèle. Voir le détail en section 2.2.

Les relations entre les principales entités sont décrites dans le modèle des relations entre entités suivant :

- Série ;
- Dossier ;
- Sous-dossier ;
- Volume ;
- Document ;
- Composant.

D'autres entités sont également comprises.

Dans le schéma, les entités - dossiers, documents, etc. - sont représentées par des rectangles. Les traits qui les relient indiquent les relations entre les entités. Chaque relation est légendée au milieu du trait, à lire dans le sens de la flèche. Chaque extrémité du trait porte un chiffre qui indique le nombre d'occurrences (*stricto sensu* la cardinalité) ; les nombres sont expliqués dans la légende. Par exemple, la figure 2.3 signifie « un document archivé est constitué d'un ou plusieurs composants » (noter le sens de la flèche).

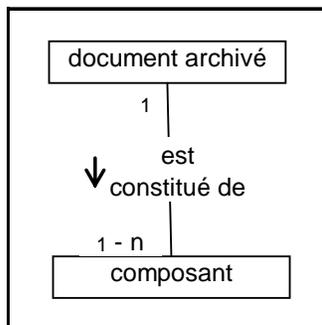


Figure 2.3

L'arc de cercle qui croise plusieurs traits ou relations indique que ces relations sont systématiquement exclusives. Par exemple l'arc de cercle de la figure 2.4 signifie « un document est stocké soit dans un volume soit dans un sous-dossier mais pas dans les deux ».

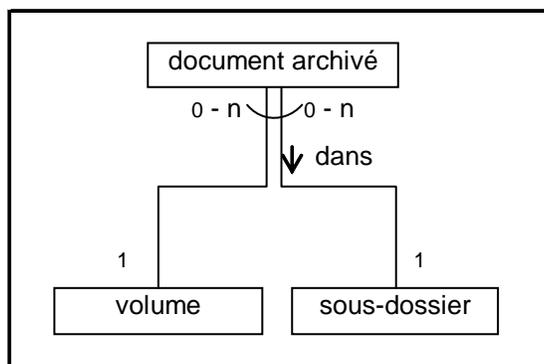


Figure 2.4

A noter que l'entité « série » est reliée à elle-même par la relation « est constituée de ». Cette relation traduit formellement la relation entre les séries d'un plan de classement hiérarchique, où une série peut être constituée d'autres séries. Si cette relation (parfois appelée relation récursive) est supprimée, le modèle s'applique aussi à des relations non-hiérarchiques.

Dans la suite du texte, les expressions [en bleu](#) indiquent qu'il s'agit de la première occurrence d'un terme du glossaire. Dans la version électronique, c'est un hyperlien vers la définition : cliquer pour atteindre la définition du glossaire et cliquer de nouveau pour revenir au texte.



# 3. plan de classement et organisation des dossiers

Ce chapitre énumère les exigences liées à la gestion du [plan de classement](#) et à l'organisation des [dossiers](#). Ce sont d'abord les exigences pour l'élaboration d'un plan de classement (section 3.1). Suivent les exigences relatives aux [séries](#) et aux dossiers (section 3.2) puis aux [volumes](#) et aux [sous-dossiers](#) (section 3.3). La section 3.4 énumère les exigences liées à la maintenance du plan de classement.

Le plan de classement est la pierre angulaire de tout [SAE](#). Il permet qu'un [document électronique](#) soit [archivé](#) et conservé avec d'autres qui éclairent son contexte en précisant comment les documents électroniques sont organisés en dossiers, ainsi que les relations entre les dossiers.

Le fait de pouvoir rattacher un document archivé directement à une série aussi bien qu'à un dossier est une différence importante entre MoReq2 et le texte antérieur. Le MoReq initial ne le permettait pas et n'autorisait que l'archivage dans un dossier.

MoReq2 permet donc de [capturer](#) un document sous :

- une série,
- un dossier,
- un sous-dossier, ou
- un volume

Les documents seront le plus souvent rattachés à des volumes ; leur capture dans des dossiers et sous-dossiers est explicitée aux points 3.3.1, 3.3.2 et 3.3.3.

La capture directe dans une série est illustrée par la figure 3.1, par l'ajout en grisé à la figure 2.1.

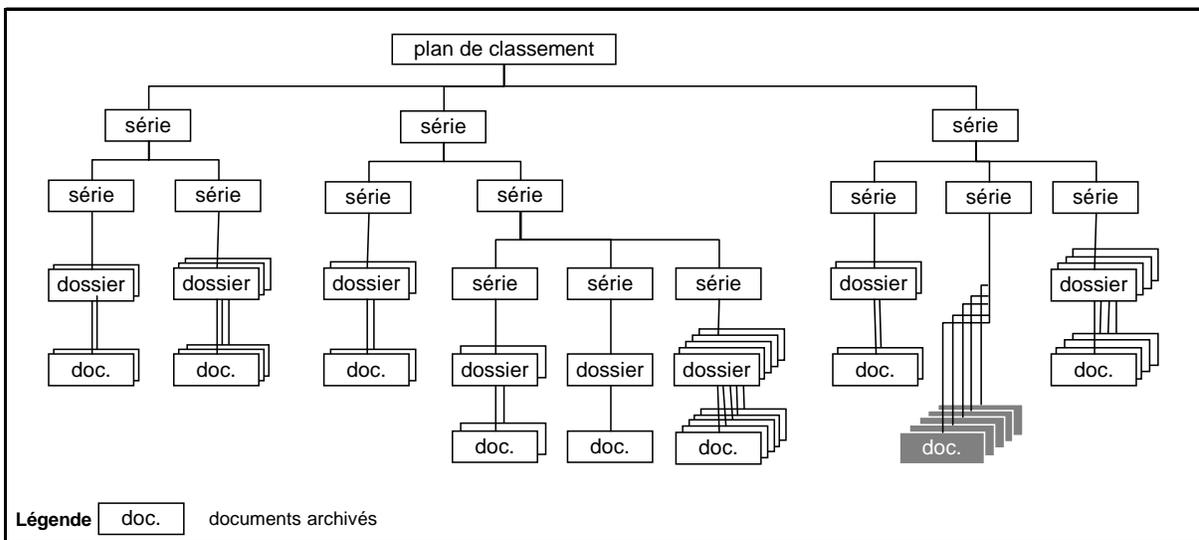


Figure 3.1

Il s'agit ici de prendre en compte les exigences de systèmes métier produisant de forts volumes à archiver. Le plan de classement hiérarchique et la constitution de dossiers restent nécessaires. Un usage inapproprié de cette possibilité risquerait de provoquer des difficultés dans la gestion ultérieure des documents, et MoReq2 recommande de n'utiliser cette fonctionnalité qu'avec circonspection. La plupart des utilisateurs de MoReq2 ne devraient pas avoir besoin de recourir à cette fonctionnalité, et MoReq2 tient à préciser qu'elle peut se révéler gênante.

La conformité à MoReq2 requiert un plan de [classement](#) hiérarchique dans la mesure où :

- les schémas hiérarchiques sont capables d'assurer une organisation efficace, stable et claire des documents archivés ;
- les modèles hiérarchiques sont largement utilisés en Europe

Ceci reste compatible avec la version précédente de MoReq. De nombreuses exigences utilisent le concept de série. Le plus souvent, il est possible d'appliquer l'exigence à un plan de classement non hiérarchique mais ce ne sera pas toujours vrai.

Il est essentiel que le plan de classement (techniquement, le plan de classement pour l'archivage) soit calqué sur les besoins métier. Les bonnes pratiques suggèrent d'organiser un plan de classement des processus métiers avant d'élaborer son plan de classement pour l'archivage.

## 3.1 CONFIGURER LE PLAN DE CLASSEMENT

---

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
3.1.1	<p>Le SAE doit intégrer et être compatible avec le plan de classement métiers.</p> <p><i>Cette exigence n'est pas testable en général ; elle figure ici comme un rappel aux utilisateurs de MoReq2 du besoin d'aligner le plan de classement géré par le SAE sur les besoins métier. Ces besoins devraient se retrouver dans l'organisation des documents à l'extérieur du SAE.</i></p>	N
3.1.2	<p>Le SAE doit maintenir son intégrité (intégrité relationnelle ou autre) en permanence, indépendamment :</p> <ul style="list-style-type: none"> <li>• des activités de maintenance ;</li> <li>• de toute autre action des <a href="#">utilisateurs</a> ;</li> <li>• des pannes des composants du système.</li> </ul> <p><i>En d'autres termes, une rupture de continuité du SAE ou de ses bases de données qui résulterait de l'action d'un utilisateur ou d'une panne logicielle doit être impossible.</i></p>	P
3.1.3	<p>Le SAE devrait permettre aux <a href="#">administrateurs</a> de doter chaque plan de classement d'un titre et d'un descriptif, et doit automatiquement attribuer un identifiant à chaque plan de classement.</p>	O

Réf	Exigence	Test
	Ces <a href="#">métadonnées</a> faciliteront les fonctions telles que l' <a href="#">export</a> des plans de classement et des documents archivés.	
3.1.4	<p>Le SAE doit être capable de supporter un plan de classement représentant des dossiers et des documents organisés en séries hiérarchisées.</p> <p><i>L'utilisation d'un plan de classement hiérarchique est obligatoire pour la conformité à MoReq2, afin de permettre l'héritage des règles de conservation/destruction ou d'autres métadonnées, et faciliter la navigation.</i></p> <p><i>Un plan de classement à trois niveaux est un minimum ; davantage de niveaux seront nécessaires dans de nombreux environnements.</i></p>	O
3.1.5	<p>Le SAE doit permettre d'attribuer la gestion du plan de classement à un seul administrateur, en liaison avec l'exigence 3.1.6.</p> <p><i>Dans la phrase ci-dessus, « gestion » renvoie aux opérations décrites aux sections 3.1 et 3.4.</i></p>	O
3.1.6	<p>Le SAE devrait permettre la gestion de séries spécifiques par des <a href="#">profils utilisateurs</a> et/ou un <a href="#">groupe</a> particulier d'utilisateurs.</p> <p><i>Dans l'exigence ci-dessus, « gestion » a le même sens que dans l'exigence précédente. Deux cas de figure sont prévus :</i></p> <ul style="list-style-type: none"> <li>• <i>les plans de classement trop larges pour être maintenus de manière centralisée (et qui de ce fait ont une gestion centralisée pour les niveaux supérieurs et une gestion décentralisée pour les niveaux inférieurs) ;</i></li> <li>• <i>les plans de classement comportant des séries pour la gestion des <a href="#">dossiers sériels</a> et nécessitant une gestion dans les unités métiers avec attribution éventuelle de privilèges aux <a href="#">utilisateurs autorisés</a>.</i></li> </ul>	O
3.1.7	<p>Le SAE ne devrait pas limiter le nombre de niveaux de la hiérarchie du plan de classement.</p> <p><i>Dans la plupart des cas, le nombre des niveaux nécessaires ne devrait pas excéder dix.</i></p>	P
3.1.8	<p>Le SAE doit permettre la création du plan de classement au <a href="#">moment de la configuration</a> afin qu'il soit prêt pour la capture et/ou l'importation des documents électroniques.</p> <p><i>Cette exigence vise à permettre l'élaboration du plan de classement pendant que le SAE est configuré, et avant sa mise en service pour l'archivage des documents.</i></p>	O
3.1.9	<p>Le SAE doit offrir un ou des mécanismes de nommage à définir par l'administrateur au moment de la configuration.</p>	O
3.1.10	<p>Le SAE devrait permettre l'insertion de notices (appelées descriptions) pour toutes les séries, dossiers, sous-dossiers et volumes.</p> <p><i>Ces libellés descriptifs ont pour but de préciser ce que doivent contenir ou ne pas contenir les séries et les dossiers, dans l'intérêt des utilisateurs.</i></p>	O

Réf	Exigence	Test
3.1.11	Si un schéma XML pour MoReq2 est publié, le SAE devra être capable d' <a href="#">importer</a> et d'exporter des documents, etc. conformément à ce schéma.	O
3.1.12	Le SAE devrait permettre l'import de tout ou partie du plan de classement, au moment de la configuration ou à un autre moment.  <i>Cette exigence vise à permettre la création d'un plan de classement pendant que la configuration du SAE est, et avant sa mise en service pour l'archivage. L'import d'une partie de plan correspond à l'ajout à un plan existant ou à la création d'un nouveau plan de classement qui n'existe pas.</i>	O
3.1.13	Quand le SAE importe tout ou partie d'un plan de classement, il doit permettre l'import des métadonnées associées, des <a href="#">règles de conservation/destruction</a> et des <a href="#">historiques des événements</a> , s'ils existent.  <i>Idéalement, le plan de classement importé aura ses métadonnées de séries et ses règles de conservation/destruction. Il peut arriver qu'ils manquent ou soient incomplets.</i>	O
3.1.14	Quand le SAE importe les métadonnées d'un plan de classement, il doit rejeter toute série dépourvue de libellé et produire un rapport d'anomalie pour l'administrateur énumérant les séries ainsi rejetées.  <i>Dans un SAE non conforme à MoReq2, on peut avoir une série sans libellé (valeur nulle) ; mais une telle série ne saurait être utilisée dans un SAE conforme à MoReq2.</i>	O
3.1.15	Quand le SAE importe les métadonnées d'un plan de classement, il doit attribuer à chaque série importée un code hiérarchique selon le choix opéré par l'administrateur parmi les possibilités suivantes : <ul style="list-style-type: none"> <li>• en suivant les mêmes règles qui s'appliqueraient pour un plan de classement créé manuellement ;</li> <li>• en conservant entièrement les codes d'origine (ce qui n'est possible que si la structure est compatible) ;</li> <li>• en ajoutant les codes d'origine aux codes du nouveau plan.</li> </ul> <i>Lorsqu'une hiérarchie importée comporte déjà des codes de séries hiérarchiques (ex : 4/6/4) il se peut que ces codes ne puissent pas être utilisés dans le SAE si la cohérence et l'unicité ne sont pas garanties.</i>  <i>Il existe de nombreux scénarios d'import, avec divers niveaux d'incompatibilité entre les plans hiérarchiques numériques. MoReq2 ne préjuge pas des résultats du choix d'une option logiquement impossible à cause d'une incompatibilité des plans.</i>  <i>Si les codes existants sont inexploitable, ils peuvent être néanmoins conservés comme métadonnée dénommée « ancien code de classement ».</i>	P

Réf	Exigence	Test
3.1.16	<p>Quand le SAE importe les métadonnées et les règles de conservation/destruction d'un plan de classement, il est impératif de les valider avec les mêmes règles que pour un plan de classement créé manuellement (voir chapitre 12). Si ce processus de validation détecte des erreurs (par exemple l'absence de métadonnées obligatoires, ou des erreurs de format), il doit le signaler à l'administrateur qui supervise l'import, en indiquant les métadonnées en cause.</p> <p><i>Dans l'idéal, le plan de classement importé aura des métadonnées (les métadonnées de séries) parfaitement conformes au modèle de métadonnées de MoReq2. D'autres fois, les métadonnées ne seront pas conformes. Dès lors, plusieurs cas de figure sont possibles (MoReq2 n'en préconise aucun) :</i></p> <ul style="list-style-type: none"> <li>• <i>l'import est complètement annulé et l'administrateur est informé des raisons de cette annulation ;</i></li> <li>• <i>l'import de la série non conforme est annulé et l'administrateur est informé des raisons de cette annulation ;</i></li> <li>• <i>l'administrateur est requis de choisir entre la correction de l'erreur et l'annulation de l'import pour la série rejetée ;</i></li> <li>• <i>l'import se poursuit en dépit de la non conformité de certaines métadonnées qui sont remplacées par des valeurs par défaut préalablement spécifiées et un rapport d'erreur est produit.</i></li> </ul> <p>Le rapport à l'administrateur n'exige pas que le processus d'import se fasse en direct ou en temps réel ; on peut admettre une opération décalée (batch).</p>	0
3.1.17	Le SAE devrait pouvoir effectuer l'export de tout ou partie du plan de classement.	0
3.1.18	Quand le SAE permet l'export de tout ou partie du plan de classement, les métadonnées associées, sélectionnées par un administrateur habilité, doivent être incluses.	0
3.1.19	Quand le SAE permet l'export de tout ou partie du plan de classement, les règles de conservation/destruction associées, sélectionnées par un administrateur, doivent être incluses.	0
3.1.20	Quand le SAE permet l'export de tout ou partie du plan de classement, l'export doit inclure tout ou partie de l'historique des événements, au choix de l'administrateur.	0
3.1.21	<p>Quand le SAE permet un export (pour une des raisons ci-dessus), il doit utiliser un procédé proprement documenté pour relier les entités entre elles.</p> <p><i>La documentation du procédé doit dire comment les documents, dossiers, séries, etc. se présentent ainsi que leurs interrelations. Voir aussi 3.1.22.</i></p>	0
3.1.22	Quand le SAE permet un export (pour une des raisons ci-dessus), il devrait exporter l'information en XML ou dans un <a href="#">format</a> ouvert normalisé équivalent.	0
3.1.23	Quand le SAE permet la copie de tout ou partie du plan de classement, les métadonnées associées doivent être incluses.	0

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
3.1.24	Quand le SAE permet la copie de tout ou partie du plan de classement, les règles de conservation/destruction associées doivent être incluses.	O
3.1.25	Le SAE doit permettre aux administrateurs d'ajouter de nouvelles séries à n'importe quel point du plan, dès lors qu'il n'y a ni dossiers ni documents à cet endroit.  <i>MoReq2 n'autorise pas la coexistence des séries et des dossiers au même niveau au sein d'une série (les dossiers et les séries ne peuvent être mêlés à un même nœud de la hiérarchie du plan de classement), car ce serait contraire aux bonnes pratiques de l'archivage.</i>	O
3.1.26	Le SAE devrait permettre l'élaboration et l'utilisation simultanée de plusieurs plans de classement.  <i>Dans la plupart des cas, un seul plan de classement pour le classement initial de tous les dossiers dans le SAE suffira. Cette exigence vise à permettre le rattachement de certains dossiers à des plans de classement différents au sein du SAE. Ceci peut être nécessaire à la suite d'une fusion entre deux entreprises ou organisations, ou lorsque les différents fonds d'une même structure requièrent des systèmes de gestion différents.</i>	O

## 3.2 SERIES ET DOSSIERS

---

Cette section énumère les exigences touchant les séries et les dossiers.

Séries et dossiers sont construits différemment. Les séries fournissent un cadre pour le classement, alors que les dossiers regroupent des documents ; les séries servent à compartimenter le plan de classement, pas les dossiers. Malgré ces différences majeures, il est utile de présenter ensemble leurs exigences communes.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
3.2.1	Le SAE doit pouvoir effectuer la capture, la maintenance et la <a href="#">restitution</a> des métadonnées pour les dossiers et les séries du plan de classement conformément au modèle de métadonnées de MoReq2.	O
3.2.2	Le SAE doit restreindre la possibilité d'ajouter des métadonnées aux dossiers et aux séries selon le modèle de métadonnées de MoReq2.	N
3.2.3	Le SAE doit proposer un mécanisme d'attribution automatique d'un <a href="#">code de classement</a> hiérarchique (lorsque que ce code n'existe pas déjà - voir 3.1.15) à toute série, dossier, sous-dossier et volume au sein du plan de classement.  <i>Voir aussi 7.1.1.</i>	O

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>3.2.4</b>	<p>Le SAE doit autoriser les utilisateurs à attribuer un titre à toute série, dossier, sous-dossier ou volume <a href="#">électronique</a>.</p> <p><i>Cette exigence s'applique aux <a href="#">dossiers non sériels</a>. Dans un environnement de dossiers sériels, un processus de nommage alternatif est nécessaire. Ceci est précisé à la section 10.5.</i></p>	0
<b>3.2.5</b>	Il doit être possible d'utiliser à la fois le code de classement et le titre du dossier, séparément ou ensemble.	0
<b>3.2.6</b>	Le SAE doit permettre à un administrateur de configurer le code de classement au moment de la configuration ou plus tard.	0
<b>3.2.7</b>	<p>Le SAE devrait permettre de configurer le code de classement à partir :</p> <ul style="list-style-type: none"> <li>• du format de l'identifiant associé à chaque niveau de la hiérarchie (numérique, alphabétique) ;</li> <li>• de la première valeur de cet identifiant pour chaque série (1, 1000) ;</li> <li>• de l'intervalle à respecter entre deux séries qui se suivent (1, 10) ;</li> <li>• de la présence ou l'absence de zéros à gauche ;</li> <li>• de tout préfixe générique (« direction/ ») ;</li> <li>• de toute extension générique (nom du pays en suffixe) ;</li> <li>• du type de séparateur entre les identifiants (« / », « - »)</li> </ul>	0
<b>3.2.8</b>	<p>Le SAE doit enregistrer les dates d'ouverture et de clôture d'une série ou d'un dossier comme métadonnées de la série ou du dossier.</p> <p><i>Les dates d'ouverture et de clôture d'une série ou d'un dossier fournissent une information contextuelle importante pour les documents qui y sont rattachés. Voir aussi 3.3.9.</i></p> <p><i>Tant qu'une série ou un dossier est <a href="#">ouvert</a>, il est possible d'y rattacher des documents. Une fois <a href="#">clos</a>, il n'est plus possible d'y capturer des documents.</i></p>	0
<b>3.2.9</b>	<p>Le SAE doit enregistrer la date de création d'une nouvelle série, d'un nouveau dossier, sous-dossier ou volume comme métadonnée de la série ou du dossier.</p> <p>Dans le cas de <a href="#">dossiers physiques</a>, la date d'ouverture peut être antérieure à la date d'enregistrement dans le SAE. Cela arrive quand un dossier papier est créé et ouvert sous forme physique, avant d'être créé dans le SAE.</p> <p><i>Dans le cas de dossiers électroniques, la date d'ouverture peut être antérieure à la date d'enregistrement dans le SAE. Cela arrive quand un dossier est importé d'un autre système dans le SAE.</i></p>	0
<b>3.2.10</b>	A l'ouverture d'une nouvelle série ou d'un nouveau dossier, le SAE doit automatiquement enregistrer comme métadonnées les attributs hérités de sa position dans le plan de classement.	0

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
	<p><i>Par exemple, si un dossier intitulé « Réunions publiques » se situe dans une série intitulée :</i></p> <p><i>Plan de développement régional : Consultation publique : Réunions publiques</i></p> <p><i>et que l'administrateur ajoute un nouveau dossier intitulé « Consultations écrites » au même niveau que « Réunions publiques », le nouveau dossier doit hériter automatiquement du préfixe « « Plan de développement régional : Consultation publique.</i></p> <p><i>A noter que les métadonnées héritées ne doivent être saisies explicitement mais récupérées implicitement. Voir le détail en annexe 9.3.</i></p>	
<b>3.2.11</b>	<p>Le SAE doit autoriser l'administrateur à modifier les valeurs héritées, dans la mesure où le modèle de métadonnée de MoReq2 le permet.</p> <p><i>Les valeurs héritées sont souvent des valeurs par défaut ou une valeur initiale. Cela peut être modifié, dès lors que le modèle de métadonnées est respecté.</i></p>	O
<b>3.2.12</b>	<p>Tout ajout aux métadonnées héritées d'une série devrait être hérité par défaut par toutes les séries et dossiers « filles/fils ».</p>	O
<b>3.2.13</b>	<p>Le SAE devrait supporter l'introduction d'un vocabulaire contrôlé conforme à ISO 2788 pour les métadonnées de séries et de dossiers, en plus des autres exigences de cette section.</p>	O
<b>3.2.14</b>	<p>Le SAE devrait supporter l'introduction d'un vocabulaire contrôlé conforme à ISO 5964 pour les métadonnées de séries et de dossiers, en plus des autres exigences de cette section.</p> <p><i>Les exigences 3.2.13 et 3.2.14 sont identiques à ceci près que la première vise les thésaurus monolingues et la seconde les thésaurus multilingues.</i></p>	O
<b>3.2.15</b>	<p>Le SAE ne doit imposer aucune limitation au nombre de séries ou de dossiers à créer.</p>	P
<b>3.2.16</b>	<p>Le SAE devrait pouvoir exporter une liste, ou un <a href="#">répertoire</a>, de tous les dossiers ou des dossiers relevant d'une série donnée (avec ses séries filles) au format XML et/ou dans un format lisible par l'homme.</p>	P
<b>3.2.17</b>	<p>Le SAE doit permettre à l'administrateur de configurer une série de façon à ce qu'elle accepte ou non qu'on y rattache directement des documents.</p> <p><i>Autrement dit, le système doit pouvoir être configuré pour que les documents ne soient pas rattachés à un dossier, sous-dossier ou volume.</i></p>	O

## 3.3 VOLUMES ET SOUS-DOSSIERS

---

Dans un système de stockage d'archives papier, il est essentiel de subdiviser les gros dossiers pour des raisons d'ergonomie et de bonne conservation physique des chemises, reliures, pochettes, etc. Par exemple, les [dossiers papier](#) sont limités à 2 cm d'épaisseur via la création de volumes. Quand le dossier (en réalité le premier volume du dossier, quoique dénommé « dossier ») atteint la taille limite - 2 cm d'épaisseur dans cet exemple - il est considéré comme clos et un nouveau volume est ouvert. Ceci n'est pas vrai pour les dossiers électroniques - un dossier électronique peut généralement grossir presque sans limite sans ce type de problème.

Toutefois, dans la pratique, il peut être avantageux d'éclater de gros dossiers électroniques en plusieurs volumes. Exemples :

- si un utilisateur doit travailler de manière distante (à cause d'une connexion à faible bande passante, ou après avoir téléchargé des documents sur son PC portable, ou sur un outil de stockage à capacité limitée) ;
- quand les dossiers ne sont jamais clos, en raison (par exemple) d'un classement géographique.

De même, les dossiers papier sont souvent divisés en sous-dossiers, particulièrement les dossiers sériels. On utilise des sous-dossiers pour structurer le contenu du dossier, souvent en lien avec le [type de document](#).

Parallèlement, il peut être avantageux de diviser les dossiers électroniques en sous-dossiers, par exemple :

- pour faciliter la navigation au sein du dossier ;
- pour donner un moyen de gérer les documents dotés d'exigences de conservation différentes au sein du dossier, tels que les documents visés par la législation sur la protection des données personnelles.

Cette section inclut les exigences relatives à l'utilisation des volumes et sous-dossiers, servant les uns et les autres à subdiviser les dossiers qui seraient plus difficilement gérables sans cela. Toutefois, MoReq2 n'impose pas la création de ces subdivisions ; il s'agit plutôt que les logiciels conformes à MoReq2 soient capables de fournir ces subdivisions si elles sont nécessaires.

*Le concept de sous-dossier n'existait pas dans la version précédente de MoReq<sup>1</sup>.*

En résumé :

- chaque dossier contient un ou plusieurs sous-dossiers ;
- chaque sous-dossier contient un ou plusieurs volumes ;
- les volumes des différents sous-dossiers sont créés indépendamment ;
- tous les sous-dossiers d'un dossier ouvert peuvent être ouverts ou clos par les utilisateurs selon les besoins ;
- dans un sous-dossier, il ne peut y avoir qu'un seul volume ouvert.

Pour plus de détail sur les sous-dossiers et les volumes, voir section 2.2.

---

<sup>1</sup> Note du traducteur : en fait, le terme de sous-dossier existe dans la traduction de MoReq1 mais il traduit le concept de volume. Il prend ici son vrai sens de division logique et non mécanique du dossier.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
3.3.1	Il doit être possible pour un administrateur, au moment de la configuration du SAE ou plus tard, de supprimer la possibilité de créer des sous-dossiers et/ou des volumes dans les dossiers du plan de classement.	0
3.3.2	Il doit être possible pour un administrateur au moment de la configuration du SAE ou plus tard de n'autoriser la création de sous-dossiers dans les dossiers que dans une zone donnée du plan de classement.	0
3.3.3	Il doit être possible pour un administrateur au moment de la configuration du SAE ou plus tard de n'autoriser la création de volumes dans les dossiers que dans une zone donnée du plan de classement.	0
	<p><i>Le but de ces trois exigences est de permettre aux entreprises/organisations d'autoriser ou d'interdire l'utilisation de sous-dossiers et/ou de volumes dans différentes parties du plan de classement. Cette possibilité procure une grande souplesse mais qui peut aussi engendrer de la complexité et de la confusion pour les utilisateurs.</i></p> <p><i>Quand une partie du plan de classement accepte les sous-dossiers, tous ses dossiers doivent contenir au moins un sous-dossier. Quand une partie du plan de classement accepte les volumes, tous ses dossiers (ou sous-dossiers) doivent contenir au moins un volume.</i></p> <p><i>L'essentiel est que le système soit transparent pour les utilisateurs, par exemple :</i></p> <p><i>quand un sous-dossier ne contient qu'un seul volume, on peut admettre que sous-dossier et volume se confondent pour l'utilisateur final ;</i></p> <p><i>quand un dossier ne contient qu'un sous-dossier qui ne contient lui-même qu'un seul volume, on peut admettre que les trois se confondent pour l'utilisateur final.</i></p> <p><i>L'idée est ici de souligner qu'un SAE ne doit pas imposer cette structure de « dossier, sous-dossier, volume ». Il doit permettre l'usage de sous-dossiers et de volumes, tout en permettant aux utilisateurs de se limiter aux dossiers si cela leur convient mieux.</i></p> <p><i>Le fondement de tout ceci est que seul l'utilisateur voit ce qui est important du point de vue des processus métier et n'est pas embarrassé par des choix pouvant prêter à confusion.</i></p>	
3.3.4	Le SAE doit prendre en compte le concept de volume électronique ouvert et clos comme suit : <ul style="list-style-type: none"> <li>• seul le volume le plus récemment créé dans un sous-dossier peut être ouvert ;</li> <li>• tous les autres volumes de ce sous-dossier doivent être clos.</li> </ul>	0
3.3.5	Le SAE doit empêcher un utilisateur d'ajouter un document électronique à un volume clos.	0

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>3.3.6</b>	Le SAE doit permettre à l'administrateur d'ajouter un volume électronique à n'importe quel sous-dossier électronique qui n'est pas clos.  <i>Le processus d'ajout d'un nouveau volume consiste à clore le volume courant et à créer un nouveau volume, ouvert.</i>	0
<b>3.3.7</b>	Le SAE doit permettre à l'administrateur d'ajouter un sous-dossier électronique à n'importe quel dossier électronique qui n'est pas clos.	0
<b>3.3.8</b>	Le SAE doit permettre aux utilisateurs de <a href="#">clore</a> un sous-dossier à tout moment.	0
<b>3.3.9</b>	Le SAE doit enregistrer la date d'ouverture du nouveau volume ou du nouveau sous-dossier comme métadonnée.	0
<b>3.3.10</b>	A l'ouverture d'un nouveau volume ou sous-dossier, le SAE doit lui attribuer automatiquement, par héritage, les métadonnées communes du dossier, comme l'indique le modèle de métadonnées de MoReq2.  <i>Les documents archivés dans un volume doivent être accessibles, que le volume soit ouvert ou clos.</i>	0
<b>3.3.11</b>	Quand un nouveau volume est ouvert, le SAE doit automatiquement lui attribuer un identifiant qui est unique au sein de son sous-dossier.  <i>L'identifiant pourrait être une simple nombre séquentiel, recommençant à 1 pour chaque sous-dossier.</i>	P
<b>3.3.12</b>	Le SAE doit enregistrer la date de clôture des volumes et des dossiers comme métadonnées.	0
<b>3.3.13</b>	Lorsqu'il classe un document, l'utilisateur doit voir apparaître par défaut le volume le plus récemment créé dans le sous-dossier sélectionné.	0
<b>3.3.14</b>	Le SAE doit permettre la création de plusieurs sous-dossiers ouverts concomitamment au sein d'un même dossier.	0
<b>3.3.15</b>	Le SAE doit permettre à un administrateur de supprimer un volume vide.	0
<b>3.3.16</b>	Le SAE doit permettre à un administrateur de supprimer un volume vide et de ré-ouvrir le précédent volume du sous-dossier en une seule action, avec enregistrement dans l'historique des événements.  <i>Ceci doit permettre de corriger une erreur due à la clôture incorrecte d'un volume.</i>	0
<b>3.3.17</b>	Le SAE devrait permettre à l'administrateur de créer un modèle de sous-dossier pour une série donnée, qui indiquerait les sous-dossiers à créer automatiquement pour chaque nouveau dossier créé dans cette série.	0

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
	<i>Ceci vaut principalement pour les dossiers sériels. Par exemple, dans une compagnie d'assurance, le modèle pourrait indiquer, pour la série des polices d'assurance client, les sous-dossiers suivants : police et avenants, correspondance interne, correspondance avec le corps médical, facturation, autre correspondance client. Dès lors, tout nouveau dossier créé dans cette série comporterait automatiquement ces sous-dossiers.</i>	
<b>3.3.18</b>	Le SAE doit automatiquement clore tous les sous-dossiers d'un dossier si leur dossier « père » est clos.	0
<b>3.3.19</b>	Le SAE doit permettre aux utilisateurs de clore les volumes individuellement.	0

## 3.4 MAINTENANCE DU PLAN DE CLASSEMENT

---

Cette section énonce d'abord les exigences pour le reclassement, le regroupement, la division et la duplication des séries (3.4.1 to 3.4.4). Si le plan de classement est bien conçu, ces fonctionnalités ne devraient pas être utilisées. Elles visent des circonstances exceptionnelles telles que les fusions ou réorganisations, ou la correction d'erreurs, ou encore le cas où le plan de classement ne correspond plus à l'activité. Ces exigences sont à rapprocher de 9.3.3 et 9.3.4. La section s'achève par des exigences complémentaires pour la maintenance du plan de classement (à partir de 3.4.17).

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>3.4.1</b>	Le SAE doit permettre à un administrateur de reclasser une série au sein du plan de classement en une seule opération.  <i>« Reclasser » signifie ici reclasser une série ou un dossier, c'est-à-dire le déplacer à un autre point du plan de classement. Le reclassement peut se faire au même niveau ou à un autre niveau du plan. Le reclassement impose plusieurs exigences complémentaires décrites plus loin.</i>	0
<b>3.4.2</b>	Le SAE doit permettre à un administrateur de regrouper deux séries en une seule opération.  <i>Le mot « regroupement » doit s'entendre comme suit : si une série est regroupée avec une autre, les subdivisions et contenus de la première sont reclassés et deviennent les subdivisions et contenus de la seconde ; la première série est close.</i>	0
<b>3.4.3</b>	Le SAE doit permettre à un administrateur de diviser une série en deux en une seule opération.	0

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
	<p><i>Le mot « division » doit s'entendre comme suit : si une série est divisée :</i></p> <p><i>une nouvelle série est créée, « fille » de la même série « mère » que la série divisée (avec toutes les exigences de création d'une nouvelle série, notamment la capture et l'héritage des métadonnées) ;</i></p> <p><i>l'utilisateur précise à partir de quel point la série doit être divisée ;</i></p> <p><i>tous les contenus de la série au-delà de ce point (c'est-à-dire avec un code de classement de niveau plus élevé) sont reclassés dans la nouvelle série.</i></p> <p><i>Les contenus de la série divisée peuvent être de tous types : séries, dossiers ou documents.</i></p>	
<b>3.4.4</b>	<p>Le SAE devrait permettre à un administrateur de dupliquer une série du plan de classement en une seule opération.</p> <p><i>« Dupliquer » signifie ici créer une copie de la série avec tout son contenu à un autre point du plan de classement tout en laissant la série dupliquée à sa place. La copie peut se trouver au même niveau du plan de classement ou à un autre niveau. La duplication impose plusieurs exigences complémentaires décrites plus loin.</i></p> <p><i>Cette option est prévue pour la duplication de branches d'un plan de classement, opération requise par exemple lors de la conception d'un plan de classement dont la structure n'est pas fonctionnelle.</i></p> <p><i>Le recours à un export suivi d'un import ne sera pas considéré suffisamment simple pour répondre à cette exigence.</i></p>	0
<b>3.4.5</b>	<p>Quand une série est reclassée ou copiée, le SAE doit garantir que les dossiers reclassés ou copiés avec leurs contenus sont reclassés avec les codes de classement correspondant à leur nouvel emplacement dans le plan de classement.</p> <p>Ceci signifie que toute série, dossier, sous-dossier, volume, document ou <u>composant</u> reclassé ou copié reçoit un nouveau code de classement, complet et signifiant.</p> <p><i>Les règles d'attribution de nouveaux codes sont les mêmes que lors de la création de nouvelles séries, dossiers, documents, etc.</i></p>	0
<b>3.4.6</b>	<p>Le SAE ne doit pas imposer à l'administrateur qui reclasse, divise, regroupe ou duplique des séries d'effectuer des exports et imports séparés.</p> <p><i>Cette exigence vise la facilité d'utilisation ; le résultat souhaité doit pouvoir être atteint sans qu'on soit obligé d'exécuter une série d'opérations déconnectées.</i></p>	0

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>3.4.7</b>	<p>Le SAE ne doit pas permettre un reclassement ou une duplication qui générerait une structure de données contraire aux règles induites par le modèle des Relations entre Entités de MoReq2 (voir 13.2) ou figurant dans d'autres exigences. Le SAE doit interdire tout reclassement qui conduirait à :</p> <ul style="list-style-type: none"> <li>• stocker des sous-dossiers ou volumes dans une série du plan de classement configurée sans sous-dossiers ou volumes (voir 3.3.1, 3.3.2, 3.3.3) ;</li> <li>• stocker des documents directement dans une série qui contient déjà des dossiers, et vice versa ;</li> <li>• stocker des dossiers directement dans une série qui contient déjà des séries, et vice versa.</li> </ul>	O
<b>3.4.8</b>	Le SAE doit garantir que lors d'un reclassement, tous les documents électroniques restent bien attachés aux séries ou dossiers reclassés ; et que le lien avec les sous-dossiers, volumes et dossiers est maintenu.	P
<b>3.4.9</b>	Le SAE doit garantir que lors d'une duplication, toutes les copies des documents électroniques restent bien attachées aux nouvelles séries et/ou dossiers, et que les copies de sous-dossiers, volumes et dossiers sont correctement reliées.	P
<b>3.4.10</b>	En cas de déplacement ou de reclassement de séries, dossiers, volumes, sous-dossiers ou documents, les dossiers clos doivent rester clos, avec les références (codes de classement) précédant la modification.	O
<b>3.4.11</b>	<p>En cas de déplacement ou de reclassement de séries, dossiers, volumes, sous-dossiers ou documents, les dossiers ouverts doivent :</p> <ul style="list-style-type: none"> <li>• soit être fermés, avec leurs références au précédent plan de classement et l'enregistrement de la référence au nouveau dossier dans les métadonnées ;</li> <li>• soit être référencés selon le nouveau plan, avec enregistrement des références du précédent plan de classement dans les métadonnées ;</li> </ul> <p>à la discrétion de l'administrateur qui effectue le reclassement.</p>	O
<b>3.4.12</b>	<p>En cas de reclassement ou de duplication de séries, le SAE doit permettre que les séries et leurs subdivisions puissent hériter des métadonnées de la nouvelle série mère.</p> <p><i>Il s'agit notamment des habilitations et des niveaux de sécurité.</i></p>	O
<b>3.4.13</b>	<p>En cas de reclassement ou de duplication de séries, le SAE doit être capable d'appliquer les règles de conservation/destruction héritées de la nouvelle série mère aux séries reclassées ou dupliquées et à leurs subdivisions, en plus des règles de conservation/destruction existantes.</p> <p><i>Il s'agit là de la fonctionnalité minimale ; le SAE peut proposer d'autres moyens de gérer les règles de conservation/destruction.</i></p>	O

Réf	Exigence	Test
	<i>Il peut s'ensuivre des contradictions entre les règles ; le cas échéant, on se conformera aux exigences du chapitre 5.1 (voir 5.1.18 et 5.1.33).</i>	
3.4.14	En cas de reclassement ou de duplication de séries, le SAE doit demander à l'administrateur d'en saisir la raison parmi les métadonnées.  <i>La saisie d'une raison est obligatoire : reclassement et duplication étant exceptionnels, une erreur pourrait compromettre l'intégrité des documents archivés.</i>	0
3.4.15	En cas de reclassement ou de duplication de séries, dossiers ou documents, le SAE doit enregistrer leur statut précédant dans l'historique des événements.	0
3.4.16	En cas de reclassement de séries, le SAE doit enregistrer les valeurs antérieures de leurs métadonnées.  <i>Les deux exigences ci-dessus ont pour objectif de permettre d'établir l'historique des documents reclassés.</i>	0
3.4.17	Le SAE devrait permettre à un administrateur de déclarer « inactif » une série ou un dossier pour éviter que de nouveaux dossiers soient ajoutés à cette série ou de nouveaux documents à ce dossier.	0
3.4.18	Le SAE devrait permettre à un administrateur de supprimer une série vide.	0
3.4.19	Le SAE doit systématiquement empêcher la suppression d'un fichier électronique ou d'une part de son contenu.  <i>Il y a deux exceptions à cette exigence :</i> <ul style="list-style-type: none"> <li>• <i>la <u>destruction</u> en accord avec la règle de conservation/destruction - comme indiqué au point 5.1.25 ;</i></li> </ul> <i>ou</i> <ul style="list-style-type: none"> <li>• <i>la suppression par un administrateur dans le cadre d'une procédure d'audit - comme indiqué au point 9.3.</i></li> </ul>	0
3.4.20	Le SAE doit autoriser les utilisateurs à clore un dossier électronique.  <i>Ce point diffère de l'exigence correspondante de MoReq qui limitait cette action aux <u>administrateurs</u>.</i>	0

- 3.4.21** Le SAE devrait être capable de clore un volume électronique automatiquement sur la base de critères spécifiques définis lors de la configuration ; ce sera au minimum :
- des volumes délimités par la fin d'un cycle annuel ; par exemple, la fin de l'année civile, de l'année comptable ou tout autre cycle annuel prédéfini ;
  - l'écoulement d'un laps de temps depuis un événement donné, par exemple le dernier ajout d'un document électronique au volume ;
  - le nombre de documents électroniques archivés dans ce volume.
- D'autres critères peuvent être souhaitables dans certains cas, par exemple quand la taille du volume atteint la capacité de stockage d'un disque amovible..*
- 3.4.22** Le SAE doit faire en sorte que les contenus des séries, dossiers, sous-dossiers et volumes clos soient aussi aisément accessibles que ceux qui sont ouverts, sans faire de différence entre les uns et les autres.
- Autrement dit, si des utilisateurs recherchent des informations au sein du SAE, le fait que les dossiers soient clos ou ouverts doit être transparent pour eux ; les mêmes fonctionnalités de recherche et d'accès doivent s'appliquer.*
- 3.4.23** Le SAE devrait permettre aux utilisateurs de créer des références croisées (liens de type « voir aussi ») entre les dossiers. 0
- 3.4.24** Le SAE devrait permettre de créer des entrées multiples pour un document électronique archivé dans plusieurs séries, dossiers, sous-dossiers ou volumes, sans dupliquer le document ou la [pièce](#) qui le constitue. 0
- MoReq2 ne précise pas la manière de procéder. Une des façons de répondre à cette exigence peut être l'utilisation de pointeurs lors de la capture de plusieurs documents comportant la même pièce.*
- 3.4.25** Le SAE doit fournir aux administrateurs des outils de reporting pour produire des statistiques sur la vie du plan de classement, y compris le nombre et la taille des séries, dossiers, volumes, sous-dossiers et documents créés, clos ou détruits au cours d'une période donnée. 0
- Le reporting devrait être à la fois global et au niveau d'un utilisateur ou d'une série.*
- 3.4.26** Le SAE devrait fournir des fonctionnalités de reporting adaptées à la vie du plan de classement. P
- 3.4.27** Tout utilisateur travaillant sur une série, un dossier ou un document devrait pouvoir accéder à son contexte, c'est-à-dire aux métadonnées et au dossier ou à la série mère ; cet accès aux entités mères doit se faire à partir de la série, du dossier ou du document. 0
- Il doit être possible d'accéder au contexte sans quitter la série ou le dossier, de sorte que le travail en cours sur ce dossier ne soit pas interrompu.*

- 3.4.28** Si un mot-clé d'un dossier est modifié, le SAE doit demander à l'administrateur de saisir la raison de ce changement. 0
- 3.4.29** Si un mot-clé d'un dossier est modifié, le SAE doit conserver une trace de son statut antérieur afin que l'historique puisse être facilement établi. 0

*Ces contrôles de changement de mots-clés visent à minimiser le risque de dissimulation de documents via des modifications de mots-clés. Dans la mesure où les mots-clés servent à retrouver les documents archivés, il est nécessaire de tracer leurs modifications pour éviter qu'un utilisateur puisse tenter de cacher un document en modifiant ses mots-clés.*

## 4. Contrôles et sécurité

Ce chapitre regroupe les exigences liées aux différents types de contrôle de la sécurité des documents archivés. Il s'agit des fonctions visant à préserver les caractéristiques des documents archivés définies par ISO 15489 (section 7.2).

Il est essentiel de pouvoir contrôler qui est autorisé à accéder aux documents archivés et dans quelles circonstances, dans la mesure où ces documents peuvent contenir des données personnelles, commerciales ou sensibles au plan opérationnel.

Des restrictions d'accès peuvent également être nécessaires pour les utilisateurs externes. Par exemple, dans les pays où la législation sur l'accès à l'information autorise l'accès à certains documents publics, les usagers peuvent souhaiter voir ces documents. Un partage partiel de l'entrepôt du SAE avec des partenaires peut être souhaitable. Voir les exigences sur ces contrôles en 4.1.

Tout accès aux documents archivés, et toute action touchant l'archivage et les données associées doivent également être enregistrés dans l'historique des événements pour assurer l'admission en preuve et faciliter la restauration des données. Les exigences correspondantes figurent en 4.2 ; elles concernent principalement les caractéristiques d'[authenticité](#) et d'intégrité des documents archivés énoncées par ISO 15489 (section 7.2).

La sécurité des documents archivés inclut la faculté de les protéger contre une faille du système par des sauvegardes, et la possibilité de restauration des données à partir de ces sauvegardes. Ces exigences figurent en 4.3 ; elles concernent la caractéristique d'exploitabilité telle que définie par ISO 15489 (section 7.2).

Les [documents vitaux](#) sont des documents hautement critiques qui doivent être récupérés rapidement après un sinistre. Ils sont traités à la section 4.4.

### 4.1. ACCES

---

Il est nécessaire de pouvoir contrôler l'accès aux documents archivés, ce qui requiert des spécifications et une politique de sécurité : l'accès aux documents archivés est accordé sur la base de la fonction exercée par les individus dans l'entreprise/organisation. Les utilisateurs sont généralement gérés au niveau central et peuvent avoir accès en même temps à plusieurs applications du système d'information dont le SAE.

La gestion des accès au SAE via de simples permissions nominatives accordées à des individus dans telle ou telle entité n'est pas une bonne pratique. Les droits d'accès devront plutôt être accordés à des [profils](#) et/ou des groupes avec la possibilité d'archiver et de consulter les documents dans telle ou telle série ou tel ou tel dossier du plan de classement.

Outre la possibilité d'accéder à certaines parties du plan de classement, les autorisations limitent également les actions qu'un utilisateur, un profil ou un groupe peut effectuer dans le SAE : passer en revue les métadonnées ou les contenus, les modifier ou les détruire, créer ou voir des entités d'un type particulier.

Les procédures de sécurité basées sur les profils peuvent ainsi interdire à un utilisateur la recherche et la consultation des documents archivés dans certaines parties du plan de classement.

Les autorisations peuvent être accordées à des groupes et héritées par les membres du groupe. L'attribution des autorisations au niveau du groupe plutôt qu'à l'utilisateur facilite la gestion du SAE dans le temps : nouveaux utilisateurs, mutations internes, départs.

La définition de profils dans le SAE permet l'attribution automatique d'autorisations multiples à un utilisateur ou à un groupe. Lorsque l'utilisateur ou le groupe quitte ce profil, toutes les autorisations sont automatiquement retirées.

Le SAE doit pouvoir réserver la fixation de ces droits d'accès à certains profils. Dans la table figurant en 13.4., cette fonction est attribuée aux administrateurs.

A noter que, d'un point de vue système, le rôle des administrateurs se borne à mettre en œuvre la politique décidée par la direction générale. La politique de sécurité et sa déclinaison pour les utilisateurs finaux sont basées sur les besoins des métiers en termes d'accès à l'information, sur la politique d'archivage et sur l'environnement réglementaire : loi sur l'information, loi sur la sécurité des données, loi sur les archives, réglementations industrielles (voir la section 11.5).

Parfois, les autorisations d'accès au SAE sont entièrement gérées par le SAE. D'autres fois, certaines autorisations sont gérées par un logiciel externe, tel qu'un gestionnaire de réseau. Les deux sont compatibles avec les exigences ci-après.

Les profils identifiés ne sont qu'indicatifs. C'est à l'entreprise/organisation de fixer le nombre et les caractéristiques des profils nécessaires, le cas échéant, en fonction de ses propres exigences.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>4.1.1</b>	<p>Le SAE doit interdire à toute personne d'effectuer quelque action que ce soit dans le SAE à moins d'y être dûment autorisée et après s'être identifiée et authentifiée.</p> <p>MoReq2 ne précise pas la nature du mécanisme d'authentification. Le plus souvent, un identifiant utilisateur et un mot de passe constitueront un mécanisme d'authentification suffisant. Les entreprises/organisations utilisant MoReq2 pour un cahier des charges s'assureront que celui-ci inclut un niveau d'authentification approprié.</p>	O
<b>4.1.2</b>	<p>Le SAE doit permettre aux administrateurs d'accorder l'accès aux documents, sous-dossiers, dossiers, séries et métadonnées à des utilisateurs, profils et/ou <a href="#">groupes</a> donnés et pour une période donnée.</p>	O
<b>4.1.3</b>	<p>Le SAE ne doit pas limiter le nombre des profils configurables.</p>	P
<b>4.1.4</b>	<p>Le SAE doit permettre aux administrateurs de gérer les autorisations pour l'ensemble des profils et groupes. Ces autorisations précisent les fonctionnalités, les métadonnées, les documents ou dossiers auxquels les profils et groupes ont accès, ainsi que les types d'accès.</p>	O

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>4.1.5</b>	<p>Le SAE doit proposer aux administrateurs des autorisations pour :</p> <ul style="list-style-type: none"> <li>• restreindre l'accès à tels ou tels dossiers ou documents ;</li> <li>• restreindre l'accès à telle ou telle série du plan de classement ;</li> <li>• restreindre l'accès en fonction des <a href="#">niveaux d'habilitation</a> des utilisateurs (le cas échéant) ;</li> <li>• restreindre l'accès à certaines particularités ou fonctionnalités (ex : lecture, mise à jour et/ou destruction de métadonnées) ;</li> <li>• refuser l'accès après une date donnée ;</li> <li>• autoriser l'accès après une date donnée.</li> </ul> <p><i>L'attribution des autorisations d'accès devrait se conformer à la politique de sécurité.</i></p> <p><i>Le niveau de granularité requis est indiqué en 13.4.</i></p>	P
<b>4.1.6</b>	<p>Le SAE devrait permettre une configuration donnant une possibilité d'accès par le biais d'un réseau intégré.</p>	O
<b>4.1.7</b>	<p>Le SAE doit permettre aux administrateurs d'ajouter ou de retirer des utilisateurs à un profil ou un groupe à tout moment.</p> <p><i>On peut admettre que les administrateurs gèrent les groupes au moyen d'une solution de gestion d'annuaire séparée.</i></p>	O
<b>4.1.8</b>	<p>Le SAE doit permettre l'attribution à différents administrateurs de droits sur des différentes parties du plan de classement.</p> <p><i>Voir par exemple le modèle de contrôle d'accès en 13.4.</i></p>	O
<b>4.1.9</b>	<p>Le SAE doit permettre à un administrateur de marquer un utilisateur comme inactif sans le supprimer du système.</p> <p><i>On peut admettre que les administrateurs gèrent les utilisateurs au moyen d'une solution de gestion d'annuaire séparée.</i></p>	O
<b>4.1.10</b>	<p>Le SAE doit permettre aux administrateurs de définir les mêmes droits d'accès pour les profils et pour les utilisateurs.</p> <p><i>Cette fonction permet aux administrateurs de gérer un nombre limité de droits d'accès plutôt qu'un grand nombre d'utilisateurs individuels. Exemples de profils : manager, gestionnaire de plaintes, analyste financier, administrateur de base de données.</i></p>	O
<b>4.1.11</b>	<p>Le SAE doit pouvoir sélectionner les droits d'accès selon les profils d'accès.</p> <p><i>Voir les exemples en 13.4.</i></p>	O
<b>4.1.12</b>	<p>Le SAE doit autoriser un administrateur à créer et à gérer un groupe d'utilisateurs.</p>	O

Réf	Exigence	Test
	<i>Exemples de groupes : Ressources humaines, équipe de vente Nord.</i>	
4.1.13	Le SAE doit permettre qu'un utilisateur soit membre de plusieurs groupes.	0
	<i>Certains utilisateurs pourront avoir des exigences d'accès différentes pour différentes parties du plan de classement. En tout état de cause, les droits seront accordés aux groupes en fonction des besoins métier et des politiques.</i>	
4.1.14	Le SAE doit permettre aux administrateurs de créer des listes d'utilisateurs <i>ad hoc</i> pour le contrôle d'accès à tel ou tel sous-ensemble du plan de classement.	0
4.1.15	Le SAE doit réserver les fonctions système et les actions associées aux seuls administrateurs.	0
	<i>Ceci a pour but de préserver la valeur probante des documents électroniques archivés.</i>	
4.1.16	Le SAE doit réserver aux administrateurs le droit de créer des <a href="#">rôles d'utilisateur</a> et d'affecter des utilisateurs à des groupes et des profils.	0
	<i>Voir aussi section 13.4</i>	
4.1.17	Le SAE doit autoriser les propriétaires des documents à préciser quels autres utilisateurs ou groupes peuvent accéder aux documents archivés.	0
	<i>Pour le sens de « <a href="#">propriétaire</a> » dans MoReq2, voir le glossaire. Les propriétaires devraient logiquement être des administrateurs.</i>	
4.1.18	Le SAE doit réserver aux administrateurs le droit d'opérer des modifications (addition, correction et suppression) dans les <a href="#">rôles</a> pour les groupes, les profils ou les utilisateurs.	0
	<i>Ceci inclut les attributs tels que droits d'accès, privilèges, attribution de mot de passe et gestion.</i>	
4.1.19	Le SAE doit permettre aux administrateurs de créer des règles pour gérer l'accès des utilisateurs au SAE, de manière à ce que différents profils aient accès à différentes combinaisons de fonctions. Le SAE doit permettre que ces règles soient créées avec une granularité (niveau de détail) au moins égale à celle de la table des droits d'accès de la section 13.4.	0
	<i>Les entreprises/organisations n'ont pas toutes les mêmes exigences de contrôle d'accès. Il n'est donc pas pertinent de vouloir définir un modèle générique. C'est pourquoi, cette exigence se limite au niveau de détail du contrôle qu'un SAE doit offrir.</i>	
4.1.20	Le SAE doit permettre aux administrateurs de créer des profils supplémentaires à ceux du tableau en 13.4.	0
	<i>On peut envisager de définir des profils avec des droits d'accès spécifiques, par exemple : <a href="#">manager</a>, <a href="#">gestionnaire</a>, etc.</i>	

<b>4.1.21</b>	Le SAE devrait fournir une interface (API) pour procurer un accès aux documents archivés à partir d'une autre application.	N
<b>4.1.22</b>	Si un utilisateur effectue une recherche portant sur des contenus (par exemple recherche en plein texte ou en texte libre), le SAE doit exclure de la liste des résultats tout document archivé pour lequel l'utilisateur n'a pas les droits.  <i>Cette exigence vise à éviter que des utilisateurs recourent aux fonctions de recherche de contenu pour accéder à des documents auxquels ils n'ont pas droit.</i>	O
<b>4.1.23</b>	Si un utilisateur par ses requêtes ou en navigant, sans rechercher un contenu précis, tente d'accéder à un objet quelconque (document, volume, sous-dossier, dossier ou série) auquel il n'a pas le droit d'accéder, le SAE doit fournir une des réponses suivantes (à sélectionner lors de la configuration) : <ul style="list-style-type: none"><li>• ne fournir aucune information sur l'objet qui puisse fournir une indication de l'existence même de cet objet ;</li><li>• confirmer l'existence et (éventuellement) le propriétaire de l'objet (afficher son identifiant de dossier ou de document) mais ni son titre ni d'autres métadonnées ;</li><li>• afficher uniquement le titre, le type d'entité (série, document, etc.), la date de création et le propriétaire ;</li><li>• afficher le titre et les métadonnées de l'objet.</li></ul> <p>La première option rejoint l'exigence relative aux résultats de recherche de contenu (voir 4.1.22). Les trois autres offrent une alternative qui peut convenir dans certains cas ; elles sont présentées ici dans un ordre de sécurité décroissant. Elles devront être configurées par un administrateur.</p> <p>Cette exigence ne s'applique qu'aux tentatives d'accès sans recherche de contenu. Les recherches sur le contenu des documents archivés sont traitées par l'exigence 4.1.22, à rapprocher de celle-ci.</p>	O
<b>4.1.24</b>	Le SAE devrait permettre d'appliquer les réponses prévues au 4.1.23 à une série plutôt qu'à tout le plan de classement, à définir lors de la configuration ou plus tard.	O

## 4.2. HISTORIQUE DES EVENEMENTS

---

On appelle historique des événements l'enregistrement des opérations qui touchent le SAE, aussi bien les opérations effectuées par les utilisateurs ou les administrateurs que les opérations initiées automatiquement par le SAE en fonction du paramétrage. Voir la définition du glossaire à la section 13.1.

L'historique indique si les règles métiers sont respectées et donne l'assurance que les actions non autorisées sont identifiées et tracées.

A des fins de traçabilité, il est indispensable que le SAE puisse enregistrer dans l'historique toute opération induisant un traitement automatique ou semi-automatique au sein du système. La section 10.5 « Dossiers sériels » donne quelques exemples d'interfaces.

L'historique du SAE est un facteur clé pour satisfaire aux exigences de traçabilité grâce à l'enregistrement complet de toutes les opérations sur chaque document (dans le respect du niveau de sécurité de l'environnement technique).

L'historique peut produire un volume de données important si toutes les opérations sont auditées. C'est pourquoi, dans certains cas, la direction générale peut décider que certaines opérations n'ont pas lieu d'être tracées dans l'historique (après la date de la décision).

Dans de nombreux systèmes, l'historique en ligne est périodiquement transféré hors-ligne, l'historique hors-ligne pouvant être détruit quand les documents tracés sont eux-mêmes détruits ou si la politique d'archivage ou la législation le permettent.

Ce sont là des questions de politique managériale et/ou d'environnement légal et réglementaire. MoReq2 inclut donc les exigences permettant ces actions mais ne se prononce pas sur leur degré d'utilisation.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>4.2.1</b>	<p>Le SAE doit contenir un historique des événements inaltérable capable de capturer et de stocker automatiquement l'information relative à :</p> <ul style="list-style-type: none"><li>• toute opération effectuée sur tout document ou groupe de documents ou sur le plan de classement ;</li><li>• l'utilisateur qui entreprend cette opération ;</li><li>• la date et l'heure de l'opération.</li></ul>	O



<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
4.2.4	Le paramétrage de l'historique des événements doit permettre aux administrateurs de configurer les opérations à enregistrer automatiquement.	O
4.2.5	Toute modification des paramètres de l'historique doit être tracée dans l'historique.  <i>Il devrait être impossible de supprimer la trace des modifications des paramètres de l'historique sans que le SAE enregistre dans l'historique qui les a modifiés et quand.</i>	O
4.2.6	Dès que les paramètres de l'historique ont été définis, le SAE doit tracer les opérations automatiquement et conserver ces informations dans l'historique.	O
4.2.7	Le SAE doit conserver l'historique aussi longtemps que l'exige la politique d'archivage de l'entreprise/organisation.  <i>Ce sera en principe au moins la durée de vie des documents archivés. Mais d'autres procédures peuvent s'appliquer, par exemple, après un audit périodique, l'historique des événements est détruit et remplacé par un certificat d'audit.</i>	N
4.2.8	Le SAE doit consigner dans un historique toutes les opérations effectuées, individuellement ou par lot, sur les documents archivés, volumes, sous-dossiers, dossiers, séries et règles de conservation/destruction.	P
4.2.9	Le SAE doit consigner dans un historique toute modification des valeurs des métadonnées énumérées dans le modèle de métadonnées de MoReq2.	P
4.2.10	Toute annotation ou correction portée à un document archivé doit être enregistrée dans l'historique du document.	O
4.2.11	Le SAE doit automatiquement consigner dans un historique toute modification apportée aux paramètres d'administration.  <i>Par exemple, si un administrateur change les autorisations d'accès d'un utilisateur ou reconfigure l'historique.</i>	O
4.2.12	Le SAE doit garantir que les données d'historique sont disponibles en cas d'inspection, afin qu'un événement particulier puisse être identifié et que les données associées soient accessibles.	O
4.2.13	Le SAE doit inclure des fonctions qui permettent aux utilisateurs habilités, même peu familiers du système, de rechercher des informations dans l'historique.  <i>C'est une facilité de fonctionnement. Les utilisateurs peuvent être extérieurs, par exemple des auditeurs externes. Mais, pour le SAE, ce sont des utilisateurs.</i>	P
4.2.14	Le SAE doit permettre aux utilisateurs de rechercher dans l'historique la trace d'événements particuliers, d'objets (séries, documents, etc.), d'utilisateurs, groupes ou profils, de dates ou périodes de temps.	O

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
4.2.15	<p>Le SAE doit être capable d'exporter les données d'historique de documents, volumes, sous-dossiers, dossiers et séries, sans modifier cet historique dans le SAE d'aucune façon sauf pour y ajouter l'historique de l'export.</p> <p><i>Cette fonctionnalité doit par exemple permettre aux auditeurs externes d'examiner ou d'analyser l'activité du système.</i></p>	0
4.2.16	<p>Le SAE doit être capable de capturer et de stocker, le cas échéant, toute violation aux mécanismes de contrôle d'accès (tentative d'accès à un document, un volume, sous-dossier ou dossier par un utilisateur qui n'en a pas le droit).</p> <p><i>Voir en 4.1.23 des exemples de ces tentatives de violation. Ceci est sans objet quand le système est configuré pour cacher à l'utilisateur les informations pour lesquelles il n'a pas les droits.</i></p>	0

### 4.3. SAUVEGARDE ET RESTAURATION

---

La conduite des affaires et la réglementation requièrent que le SAE soit doté d'un dispositif complet de sauvegarde régulière des documents et des métadonnées. Il doit pouvoir restituer des documents perdus par suite de défaillance du système, d'accident, de violation de la sécurité, etc.

Des sauvegardes et restaurations automatiques et régulières peuvent être fournies par le SAE ou intégrées dans les fonctionnalités d'un système de gestion électronique de documents (GED), effectuées par un système de gestion de bases de données relié au SAE, ou par toute autre application. Dans cette section, « SAE » renvoie à l'une ou l'autre solution, selon l'environnement.

Les fonctions de sauvegarde et de restauration relèvent en fait davantage de la compétence de la direction des systèmes d'information (DSI) que d'un partage entre les administrateurs du SAE.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
4.3.1	<p>Le SAE doit fournir ou permettre des procédures de sauvegarde et de restauration automatiques pour une sauvegarde régulière de tout ou partie des séries, dossiers, documents, métadonnées, paramètres d'administration, et historique du SAE ; ainsi que leur restauration si nécessaire.</p>	0
4.3.2	<p>Le SAE doit permettre à l'administrateur de programmer des sauvegardes :</p> <ul style="list-style-type: none"> <li>• sur un critère de fréquence ;</li> <li>• selon un choix de séries, dossiers ou documents à sauvegarder ;</li> <li>• en fonction des supports de stockage, du système ou de la localisation des fichiers sauvegardés (stockage hors-ligne, système distinct, site distant).</li> </ul>	0
4.3.3	<p>Le SAE doit réserver aux seuls administrateurs autorisés la possibilité d'effectuer des restaurations à partir des sauvegardes.</p>	0

Réf	Exigence	Test
4.3.4	<p>Quand un SAE opère une restauration à partir d'une sauvegarde, l'intégrité des données et de l'historique des événements doit être préservée.</p> <p><i>Les documents archivés dûment détruits mais encore présents dans la sauvegarde ne doivent pas être restaurés, sauf cas exceptionnel.</i></p>	P
4.3.5	<p>Si le SAE prévoit des points de contrôle et des moyens de restauration progressive, le SAE doit réserver aux seuls administrateurs autorisés le droit de le faire.</p>	P

## 4.4. DOCUMENTS VITAUX

---

Les documents vitaux sont les documents archivés considérés comme indispensables à l'entreprise/organisation pour poursuivre son activité, à court et/ou long terme (voir le glossaire). Leur criticité tient soit au besoin de réagir à une situation d'urgence ou à un sinistre, soit à la protection à long terme des intérêts juridiques et financiers.

L'identification et la protection de ces documents sont particulièrement importantes et ce sont vraisemblablement ces documents-là qui devront être restaurés en premier en cas de sinistre.

Les documents archivés peuvent être vitaux pour l'ensemble de la structure, ou pour une partie des services.

Réf	Exigence	Test
4.4.1	<p>Le SAE doit permettre aux administrateurs de signaler tels et tels dossiers ou documents comme étant ou contenant des « documents vitaux ».</p> <p><i>Cette information devrait figurer en tant que métadonnée.</i></p>	O
4.4.2	<p>Le SAE doit pouvoir effectuer deux opérations de sauvegarde distinctes :</p> <ul style="list-style-type: none"> <li>• une sauvegarde « intégrale » de toutes les données du SAE (à définir);</li> <li>• une sauvegarde « vitale » circonscrite aux données de configuration et aux dossiers et documents signalés comme « vitaux ».</li> </ul> <p><i>On distingue deux opérations de sauvegarde pour les raisons suivantes :</i></p> <ul style="list-style-type: none"> <li>• <i>pouvoir programmer les sauvegardes « vitales » plus souvent que les sauvegardes « intégrales » ;</i></li> <li>• <i>permettre les sauvegardes « vitales » sur des supports différents avec un stockage distinct (et si possible plus sécurisé) que les sauvegardes « intégrales ».</i></li> </ul>	O

Réf	Exigence	Test
	<p><i>Cela permet aussi une meilleure gestion des restaurations du SAE car les restaurations « vitales » peuvent être indépendantes et intervenir à un autre moment que les restaurations « intégrales ».</i></p> <p><i>La section 4.3 précise que les sauvegardes peuvent être effectuées soit par le SAE soit par le biais d'un autre outil.</i></p>	
4.4.3	<p>Après une restauration « vitale », le SAE doit être totalement opérationnel.</p> <p><i>Après une restauration « vitale », il manquera de nombreux dossiers et documents. Malgré tout, le SAE ne doit aucunement être limité dans son fonctionnement et dans les services rendus aux utilisateurs.</i></p>	P
4.4.4	<p>Le SAE devrait proposer deux méthodes de restauration à partir d'une sauvegarde « intégrale » :</p> <ul style="list-style-type: none"><li>• restauration dans un environnement « propre » : les données restaurées effacent et remplacent les données du SAE pendant l'opération de restauration ;</li><li>• restauration dans un environnement existant : les données restaurées sont fusionnées dans l'environnement initial du SAE.</li></ul> <p><i>La première méthode de restauration est courante là où on ne pratique pas de sauvegarde « vitale ». La seconde vise le cas où un SAE a déjà été partiellement restauré à partir d'une sauvegarde « vitale » et a retrouvé son fonctionnement normal ; il est alors nécessaire de fusionner les données avec la sauvegarde « intégrale », sans réécriture des dossiers et documents vitaux préalablement restaurés ou de toute nouvelle entité qui aurait été ajoutée, ni modification du SAE depuis le moment où il a retrouvé son fonctionnement normal.</i></p> <p><i>Si le SAE permet les deux méthodes de restauration à partir de la sauvegarde « intégrale » décrite en 4.4.4, la sauvegarde « vitale » (si elle existe) sera toujours restaurée la première. La restauration « vitale » après une restauration « intégrale » n'a pas d'intérêt.</i></p> <p><i>En cas de restauration du système en deux phases comme ci-dessus, les administrateurs peuvent être amenés à opérer manuellement pour résoudre certains problèmes. Le plan de classement peut être altéré dans une sauvegarde et pas dans une autre, etc.</i></p>	O
4.4.5	<p>Le SAE doit permettre aux administrateurs d'indiquer que tels ou tels dossiers ou documents archivés ne sont plus vitaux. Cette action doit être tracée dans l'historique.</p> <p><i>Par exemple, un bail ou un contrat peuvent arriver à expiration et dès lors perdre leur caractère vital.</i></p>	O

## 5. conservation et destruction

Ce chapitre traite des exigences liées à l'utilisation de règles de conservation/destruction pour piloter le sort final des documents archivés. Ces règles indiquent la durée pendant laquelle les documents doivent être conservés dans le SAE et les modalités de sortie du système. Les exigences liées aux règles de conservation/destruction sont énumérées à la section 5.1 ; une définition figure dans le glossaire.

Les opérations à mener à l'échéance indiquée par les règles de conservation/destruction sont décrites à la suite. Les exigences pour la révision sont données en 5.2, et les exigences concernant les transferts, les exports et la destruction figurent en 5.3.

Il est dit au point 2.2 « Dossier, sous-dossier et volume électronique » que les documents archivés peuvent être organisés en séries, dossiers, sous-dossiers et volumes, en fonction des besoins métier. Selon les cas, les règles de conservation/destruction s'appliquent aux séries, aux dossiers et/ou aux sous-dossiers et/ou aux volumes. Ils peuvent aussi s'appliquer aux [types de documents](#), par exemple pour attribuer une durée de conservation courte aux données personnelles sensibles, ou une durée de conservation longue aux dessins d'ingénierie. L'arbitrage entre les règles de conservation/destruction contradictoires est prévu.

MoReq2 introduit le concept de « gel de destruction » qui ne figurait pas dans la version initiale. Les gels de destruction font suite à des événements imprévus pour empêcher la destruction de certains documents. Le but est de s'assurer que les documents archivés susceptibles d'être produits comme preuve dans une procédure juridique ne sont pas détruits machinalement en application d'une règle existante.

### 5.1 REGLES DE CONSERVATION/DESTRUCTION

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
5.1.1	Le SAE doit permettre aux administrateurs, et à eux seuls, de créer et de gérer les règles de conservation/destruction.	O
5.1.2	Le SAE ne doit pas limiter le nombre de règles de conservation/destruction.	P
5.1.3	Le SAE devrait pouvoir organiser les règles de conservation/destruction dans une structure hiérarchique proche de la structure des règles de conservation/destruction générales ou spécifiques issues du cadre réglementaire.  Une structure hiérarchique facilite la gestion d'un grand nombre de règles de conservation/destruction.	N
5.1.4	Le SAE doit attribuer à chaque règle de conservation/destruction créée un identifiant unique.	O
5.1.5	Le SAE doit s'assurer que le titre de chaque règle de conservation/destruction est unique.	O

Réf	Exigence	Test
5.1.6	Le SAE doit conserver la trace inaltérable (historique des événements) des modifications et suppressions de règles de conservation/destruction, y compris la date et l'auteur des modifications ou suppressions.	0
5.1.7	Le SAE doit s'assurer que toute correction apportée à une règle de conservation/destruction est immédiatement appliquée à toutes les entités auxquelles cette règle est associée.	0
5.1.8	Le SAE doit exiger de l'administrateur qui modifie ou supprime une règle de conservation/destruction d'en saisir la raison, et conserver cette donnée dans l'historique.  <i>Les modifications et suppressions de règles de conservation/destruction doivent être contrôlées soigneusement pour réduire le risque de destruction intempestive des documents archivés.</i>	0
5.1.9	Le SAE doit être capable d'importer et d'exporter des règles de conservation/destruction.	P
5.1.10	Le SAE doit s'assurer que toute série, tout dossier, sous-dossier et volume a au moins une règle de conservation/destruction.  <i>Cette exigence vise à ce qu'aucune entité ne soit créée sans règle de conservation/destruction ; et à améliorer l'exploitabilité.</i>	0
5.1.11	Les règles de conservation/destruction appliquées par défaut à toute nouvelle série, tout nouveau dossier, sous-dossier ou volume devraient s'hériter de l'entité mère.  <i>Si ce n'est pas possible (séries supérieures du plan de classement ou si aucune règle ne peut s'hériter - voir 5.1.18), une règle de conservation/destruction devrait s'appliquer par défaut.</i>	0
5.1.12	Tout document archivé directement dans une série doit toujours avoir au moins une règle de conservation/destruction.	0
5.1.13	La règle de conservation/destruction appliquée par défaut à tout nouveau document archivé directement dans une série (voir 3.2) doit être héritée de la série mère.	0
5.1.14	Le SAE doit permettre à un administrateur d'appliquer une règle de conservation/destruction à une série, à un dossier, sous-dossier, volume ou document à tout moment.  <i>L'expression « à tout moment » signifie qu'un administrateur peut remplacer une règle de conservation/destruction ou (si le système gère de nombreuses règles de conservation/destruction, voir 5.1.16) ajouter une règle de conservation/destruction supplémentaire à une série, à un dossier, sous-dossier, volume ou type de document. Exemple : remplacement d'une règle de conservation/destruction par défaut ; ou ajout d'une règle de conservation/destruction à la suite d'un audit. Ceci peut générer des contradictions entre les règles de conservation/destruction : voir 5.1.23.</i>	0

Réf	Exigence	Test
5.1.15	<p>Le SAE devrait pouvoir appliquer une règle de conservation/destruction par défaut aux types de documents.</p> <p><i>Ceci suppose qu'il existe des types de documents sans règle de conservation/destruction spécifique. En fait, chaque document archivé aura au moins une règle de conservation/destruction vu qu'il appartient à un dossier ou une série et que l'exigence 5.1.10 stipule qu'au moins une règle de conservation/destruction s'applique à tout dossier et toute série.</i></p>	0
5.1.16	<p>Le SAE doit permettre la coexistence de plusieurs règles de conservation/destruction pour toute série, dossier, sous-dossier ou volume.</p> <p><i>Ceci est nécessaire pour gérer des situations réelles qui mêlent des exigences de conservation issues de diverses contraintes réglementaires et de besoins métier. En voici un exemple parmi d'autres : un dossier n'est visé que par une seule règle de conservation/destruction, découlant des besoins métier car les documents de ce dossier ne sont soumis à aucune durée de conservation légale ou réglementaire. La même règle s'applique à de nombreux autres dossiers. A un moment, il s'avère nécessaire de conserver ce dossier plus longtemps que la durée initialement préconisée, en raison d'un problème métier lié à la sécurité. A ce moment-là, il apparaît que le contenu du dossier peut être soumis à un contrôle réglementaire en application des règles de sécurité ; ce qui conduit à ajouter une seconde règle de conservation/destruction au dossier. Il peut s'avérer plus tard que le problème de sécurité n'existe plus ; dès lors, la seconde règle peut être supprimée, laissant la règle initiale seule en vigueur.</i></p>	0
5.1.17	<p>La durée de conservation et le sort final de tout document archivé doivent être pilotés par les règles de conservation/destruction associées aux séries, dossiers, sous-dossiers, volumes et types de document dont relève le document, sans oublier le cas échéant un gel de destruction (voir 5.1.34).</p> <p><i>Dès qu'une règle de conservation/destruction est en vigueur, elle pilote la conservation et le sort final des documents associés à l'entité visée (sauf si d'autres règles de conservation/destruction ont la préséance).</i></p>	0
5.1.18	<p>Le SAE doit permettre l'héritage de toute règle de conservation/destruction et de ses modifications, suivant l'arborescence du plan de classement, à la discrétion de l'administrateur.</p> <p>Le choix par l'administrateur de l'héritage ou non d'une règle de conservation/destruction peut se faire par tout moyen approprié. MoReq2 ne définit pas les modalités de cette opération. Ce peut être :</p> <ul style="list-style-type: none"> <li>• la sélection de l'option au moment de la création de la règle de conservation/destruction (auquel cas elle s'applique systématiquement) ;</li> <li>• la sélection de l'option au moment où la règle est appliquée (elle s'applique alors à toutes les entités filles) ;</li> <li>• la sélection de l'option au moment de la création d'une entité (possibilité d'hériter de la règle de l'entité mère).</li> </ul>	0

Réf	Exigence	Test
5.1.19	<p>Chaque règle de conservation/destruction doit inclure :</p> <ul style="list-style-type: none"> <li>• une durée de conservation (5.1.25) et un événement déclencheur (5.1.25) ;</li> </ul> <p>ou</p> <ul style="list-style-type: none"> <li>• une date de sort final.</li> </ul>	0
5.1.20	<p>Chaque règle de conservation/destruction doit inclure :</p> <ul style="list-style-type: none"> <li>• un sort final (5.1.24) ;</li> <li>• une motivation.</li> </ul>	0
5.1.21	<p>Chaque règle de conservation/destruction devrait inclure :</p> <ul style="list-style-type: none"> <li>• une description ;</li> <li>• une référence.</li> </ul> <p><i>La référence précise la justification de la règle de conservation/destruction. C'est en général un texte de loi, une réglementation, une procédure interne.</i></p>	0
5.1.22	<p>Quand la durée de conservation applicable à des documents archivés du fait de la règle de conservation/destruction arrive à échéance, le SAE doit déclencher automatiquement le processus de décision du sort final.</p> <p><i>Ceci peut signifier que la décision est exécutée automatiquement (voir 5.2.4) ou qu'un administrateur doit intervenir (voir 5.1.23). Certaines entreprises ou organisations préfèrent la seconde approche à cause des risques liés à une destruction automatique.</i></p>	0
5.1.23	<p>Quand le SAE déclenche une décision de sort final (voir 5.1.22), si d'autres règles de conservation/destruction, avec des durées différentes ou des sorts finaux différents sont également applicables, il s'ensuit une contradiction. En pareil cas, le SAE doit être capable d'alerter automatiquement l'administrateur pour qu'il résolve la contradiction en indiquant quelle règle a la préséance.</p> <p><i>L'expression « doit être capable... » signifie que les administrateurs n'ont pas à intervenir dans tous les cas. On peut concevoir que le SAE résolve une contradiction de manière automatique ; mais il doit être possible de configurer le SAE pour demander une intervention humaine en cas de contradiction.</i></p> <p><i>Les causes d'une contradiction sont :</i></p> <ul style="list-style-type: none"> <li>• certaines règles de conservation/destruction indiquent que le sort final doit être déclenché et d'autres indiquent le contraire ;</li> </ul> <p><i>et/ou</i></p> <ul style="list-style-type: none"> <li>• différentes règles de conservation/destruction indiquent des sorts finaux différents.</li> </ul> <p><i>Dans la plupart des cas, il sera facile de déterminer quelle règle a la préséance.</i></p>	0

<b>Réf</b>	<b>Exigence</b>	<b>Test</b>
------------	-----------------	-------------

*Ces contradictions se rattachent à deux scénarios :*

- *les règles contradictoires s'appliquent toutes à la totalité d'un groupe de documents (par exemple un dossier) ;*
- *les règles s'appliquent à la fois au groupe et à certains documents dans le groupe (à certains types de documents faisant partie du groupe).*

*L'intervention d'un administrateur peut être requise lorsque la contradiction ne peut pas être résolue correctement par l'énoncé d'une instruction. Par exemple :*

- *deux règles de conservation/destruction, issues de deux contextes réglementaires distincts peuvent indiquer des durées de conservation différentes. En général, on décidera de conserver les documents pendant la durée la plus longue ;*
- *une règle de conservation/destruction peut indiquer une date de destruction pour certains documents (pour des raisons de protection des données personnelles notamment). Si cette date est antérieure à l'échéance de la durée de conservation issue d'une autre règle, la décision dépendra du poids relatif des deux exigences réglementaires.*

*Ces situations peuvent se produire quand un document relève d'un type de document appelant l'application ou l'héritage d'une règle de sort final liée au type de document plutôt qu'au groupe qui contient ce document.*

*La décision de l'administrateur peut être :*

- *de retirer une ou plusieurs des règles contradictoires du groupe ou des documents concernés*
- *de modifier une ou plusieurs des règles contradictoires pour régler la question ;*
- *de supprimer toutes les règles contradictoires et d'en appliquer une nouvelle ;*
- *d'utiliser la fonction de suppression exceptionnelle citée au point 9.3.*

*Ces actions, si elles ne sont pas rigoureusement contrôlées, peuvent faire échouer la bonne maîtrise de l'archivage. C'est pourquoi, les modifications de règles de conservation/destruction et les suppressions de documents doivent faire l'objet de procédures écrites. Dans certains cas, d'autres contrôles, du type division des tâches, seront pertinents.*

*Si la résolution de la contradiction conduit à maintenir un document dans un groupe qui sans cela n'aurait pas été conservé, on peut aussi avoir besoin de directives relatives à son stockage. On peut alors soit laisser le groupe en place, soit reclasser les documents restants (voir le point 3.4).*

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>5.1.24</b>	<p>Le SAE doit permettre au minimum les actions de sort final suivantes (voir 5.1.19) pour toute règle de conservation/destruction :</p> <ul style="list-style-type: none"> <li>• conservation permanente ;</li> <li>• révision ;</li> <li>• destruction automatique ;</li> <li>• destruction après validation par un administrateur ;</li> <li>• transfert aux archives historiques ou dans un autre centre (voir le glossaire).</li> </ul> <p><i>L'option de « destruction automatique » proposée ci-dessus peut présenter des risques ; les entreprises/organisations devront évaluer ces risques au regard des bénéfices de l'automatisation.</i></p>	O
<b>5.1.25</b>	<p>Le SAE doit permettre au minimum les combinaisons suivantes entre événements déclencheurs et durées de conservation (voir 5.1.19) :</p> <ul style="list-style-type: none"> <li>• écoulement d'un certain laps de temps après l'ouverture de la série, du dossier, sous-dossier ou volume ;</li> <li>• écoulement d'un certain laps de temps après la clôture de la série, du dossier, sous-dossier ou volume ;</li> <li>• écoulement d'un certain laps de temps après le classement du document le plus récent dans la série, le dossier, sous-dossier ou volume ;</li> <li>• écoulement d'un certain laps de temps après la consultation d'un document dans la série, le dossier, sous-dossier ou volume ;</li> <li>• écoulement d'un certain laps de temps après tel événement extérieur (événement précisé dans la règle et notifié au SAE par un administrateur plutôt que de manière automatique) (par exemple, « ... après la signature du contrat » ou « ... 100 ans après la naissance »)</li> <li>• « permanent » pour indiquer une conservation à long terme.</li> </ul> <p><i>Bien que cette liste soit a priori exhaustive, il se peut qu'une entreprise/organisation veuille ajouter d'autres événements déclencheurs ou d'autres types de durées.</i></p> <p><i>Le nombre d'événements extérieurs liés aux différentes règles de conservation/destruction n'est pas limité.</i></p>	O
<b>5.1.26</b>	<p>Le SAE ne doit pas limiter la longueur des durées de conservation.</p>	P
<b>5.1.27</b>	<p>Le SAE doit pouvoir gérer des durées de conservation d'au moins cent ans (voir 5.1.24).</p>	P

Réf	Exigence	Test
	<i>Cette durée maximum est arbitraire et équivaut en fait à ne fixer aucune limite. Même s'il est peu probable qu'un SAE existe encore dans cent ans, une exigence de cette nature permettra de transférer les documents archivés dans les systèmes à venir sans avoir besoin de réviser les règles de conservation/destruction.</i>	
5.1.28	Le SAE doit pouvoir réserver aux administrateurs la gestion du processus de sort final.	0
5.1.29	Le SAE doit enregistrer toute opération de sort final automatique dans l'historique et le notifier à un administrateur	0
5.1.30	Le SAE doit notifier systématiquement à un administrateur toute révision arrivée à échéance.	0
5.1.31	Le SAE doit permettre à un administrateur de déléguer l'exécution d'une action de révision à une autre personne.	0
5.1.32	Le SAE doit permettre à un administrateur de corriger n'importe quelle règle de conservation/destruction (sauf son identifiant unique, voir 5.1.6).	0
5.1.33	<p>Quand un administrateur déplace des documents ou des dossiers électroniques d'une série du plan de classement à une autre, le SAE doit permettre le choix suivant :</p> <ul style="list-style-type: none"> <li>• remplacer la règle de conservation/destruction initiale par la règle de la série de destination ;</li> </ul> <p>ou</p> <ul style="list-style-type: none"> <li>• donner la possibilité à l'administrateur de sélectionner la règle de conservation/destruction qui convient.</li> </ul> <p><i>Ceci fait référence au déplacement exceptionnel de documents archivés (voir 9.3.3 et 9.3.4). Lorsqu'ils utiliseront cette fonctionnalité, a priori rarement, les administrateurs devront faire très attention à la définition ou à la modification des règles de conservation/destruction, particulièrement pour les documents vitaux.</i></p>	0
5.1.34	Le SAE doit permettre à un utilisateur habilité de geler la destruction d'une série, d'un dossier, sous-dossier ou volume.	0
5.1.35	Une action de gel ne doit pas interrompre l'écoulement de la durée de conservation.	P
	<i>En tout état de cause, voir 5.1.36.</i>	
5.1.36	Le SAE doit empêcher toute suppression ou toute décision de sort final d'une entité gelée, ainsi que de ses subdivisions (entités filles) s'il y en a.	0
	<i>La suppression est décrite à la section 9.3.</i>	
5.1.37	Le SAE doit réserver le droit de suspendre un gel à un utilisateur habilité.	0

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
5.1.38	Lorsqu'un utilisateur habilité déclenche ou suspend un gel, le SAE doit capturer et stocker les informations suivantes, au minimum dans l'historique mais de préférence dans les métadonnées : <ul style="list-style-type: none"> <li>• la date de déclenchement ou de suspension du gel ;</li> <li>• l'identité de l'utilisateur habilité ;</li> <li>• le motif du gel.</li> </ul>	0
5.1.39	Le SAE devrait permettre à un utilisateur habilité de déclencher en une seule opération plusieurs gels, obéissant au même motif, sur un groupe de séries, sous-dossiers, sous-dossiers ou volumes.  <i>Cette exigence permet à un utilisateur autorisé de geler plusieurs séries, dossiers, etc. avec un même motif.</i>	0
5.1.40	Le SAE devrait permettre la levée simultanée de gels multiples (basés sur le même motif) en une seule opération, effectuée par un utilisateur habilité.	0
5.1.41	Le SAE devrait permettre qu'une série, un dossier, sous-dossier ou volume soit l'objet de plusieurs gels simultanés, parce que le gel vise cette entité, et/ou parce que le gel vise une entité supérieure. Dans les deux cas les restrictions de sort final ou autres imposées par le gel doivent être maintenues jusqu'à la levée complète du dernier gel.	0
5.1.42	Le SAE devrait permettre à un utilisateur habilité d'effectuer une recherche ou une requête sur toutes les entités visées par une opération de gel.	0
5.1.43	Le SAE devrait permettre à un utilisateur habilité de créer, de modifier ou de supprimer un message rappelant aux utilisateurs l'existence d'un gel donné à une date donnée.	0

## 5.2 REVISION DU SORT FINAL

---

Il arrive que les règles de conservation/destruction s'appliquent sans révision. Mais en général, les règles de conservation/destruction exigent une révision du sort final du groupe de documents qui a atteint la date ou l'événement indiqué dans la règle. La révision peut se baser sur les métadonnées, le contenu ou les deux pour conclure au sort final (prolongation de la durée, transfert dans un autre système, destruction ou décision mixte)

Le sort final de certains documents dépend de la législation et de la réglementation. La révision du sort final doit se faire en cohérence avec ces textes, et tenir compte aussi de la politique de tri et des procédures élaborées par l'entreprise/organisation. Le cas échéant, cette révision se fera en coordination avec l'autorité archivistique référente (visa obligatoire dans certains cas). Le détail de ces questions dépasse le cadre de MoReq2.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
------------	-----------------	-------------

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
5.2.1	Le SAE devrait notifier systématiquement à un administrateur toutes les règles de conservation/destruction arrivées à échéance à une date donnée.	0
5.2.2	Le SAE doit aider au processus de révision en présentant les séries, dossiers, sous-dossiers et volumes arrivés à échéance avec leurs métadonnées et les règles de conservation/destruction associées.  <i>Concrètement, ceci suppose des fonctions de navigation au sein des dossiers, entre les dossiers et parmi les métadonnées des dossiers et des documents.</i>	0
5.2.3	Le SAE doit pouvoir maintenir les liens entre les différentes <a href="#">conversions</a> d'un même document et permettre l'application du sort final en même temps sur toutes.	0
5.2.4	Le SAE doit permettre, lors de la révision du sort final, d'effectuer une des actions suivantes sur chaque série, dossier, sous-dossier ou volume pendant la révision : <ul style="list-style-type: none"> <li>• destruction, immédiatement ou plus tard (voir 5.3) ;</li> <li>• transfert (voir 5.3), immédiatement ou plus tard ;</li> <li>• nouvelle révision, immédiatement ou plus tard ;</li> <li>• conservation illimitée.</li> </ul> <i>Ceci peut se faire en utilisant plusieurs règles de conservation/destruction ou d'une autre façon.</i>	0
5.2.5	Le SAE doit enregistrer systématiquement la date d'une révision.	0
5.2.6	Le SAE doit permettre, lors de la révision, de saisir des commentaires dans les métadonnées des séries, dossiers, sous-dossiers ou volumes pour tracer ses décisions.	0
5.2.7	Le SAE doit conserver un historique inaltérable de toutes les décisions prises par celui qui effectue la révision, motifs compris.  <i>Les décisions doivent figurer dans les métadonnées et si possible dans l'historique.</i>	0
5.2.8	Le SAE devrait alerter l'administrateur dans le cas contradictoire où un dossier prêt à être détruit est lié à un autre dossier. Le processus de destruction doit alors être différé afin de permettre une des actions correctives suivantes : <ul style="list-style-type: none"> <li>• confirmation de la poursuite ou annulation du processus par l'administrateur ;</li> <li>• production d'un rapport détaillé sur les dossiers et documents en cause, avec les références ou les liens concernés.</li> </ul>	0

## 5.3 TRANSFERT, EXPORT ET DESTRUCTION

---

Les entreprises/organisations peuvent avoir besoin de déplacer les documents archivés dans le SAE vers un autre lieu ou système, à des fins historiques ou autres. Cette opération s'appelle « transfert ».

Les raisons d'un transfert sont notamment :

- conservation permanente des documents pour des raisons légales, administratives ou de recherche ;
- le recours à des services dédiés ou externes pour le stockage des documents archivés à moyen ou long terme.

Cela se traduit le plus souvent par un transfert des documents vers un autre SAE.

On utilise le terme transfert bien que, au départ, ce soit une copie qui est envoyée vers un autre lieu ou système. Les documents stockés initialement dans le SAE y restent et ne sont détruits qu'après vérification de la réussite du transfert.

Le terme export, quant à lui, renvoie au fait de produire une copie de **groupes de documents** complets, de dossiers et de documents pour un autre système, tout en maintenant les documents dans le système d'origine ; ils ne sont pas supprimés.

En fait, le transfert se déroule en deux temps : export de la copie avec toutes les métadonnées associées et l'historique ; puis destruction des données d'origine.

Quoi qu'il en soit, l'exigence est de bien contrôler l'exécution du transfert, de l'export ou de la destruction. Les métadonnées et l'historique doivent faire l'objet d'une décision en même temps que sont traités les documents correspondants.

Dans ce contexte, « destruction » doit être distingué de « suppression ». La suppression des documents archivés, plus généralement, est traitée au point 9.3.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>5.3.1</b>	Lorsqu'un schéma XML pour MoReq2 aura été publié <sup>1</sup> , le SAE devra être capable d'exporter les documents archivés dans un format conforme à ce schéma.  <i>Voir aussi l'exigence 6.2.1 sur les imports par lots. La prise en compte de ces deux exigences répond au besoin d'interopérabilité des SAE conformes à MoReq2.</i>	P
<b>5.3.2</b>	Si un SAE transfère ou exporte un document, il doit transférer ou exporter tous ses composants en préservant correctement le lien qui les unit.	P
<b>5.3.3</b>	Le SAE doit inclure une procédure très précise de transfert des documents, avec leurs métadonnées et les données d'historique, vers un autre système ou vers un tiers.	P

---

<sup>1</sup> Au moment où nous écrivons, il est prévu de développer un schéma XML pour MoReq2. Voir [http://ec.europa.eu/transparency/archival\\_policy](http://ec.europa.eu/transparency/archival_policy) pour plus de détail.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
5.3.4	<p>Le SAE devrait être capable d'exporter des documents avec leurs métadonnées sous la forme d'un paquet d'information à verser (SIP) tel que le définit la norme OAIS.</p> <p><i>Voir l'exigence équivalente pour les paquets d'information diffusés en 11.7.12.</i></p>	O
5.3.5	<p>Tout transfert d'une série, d'un dossier, sous-dossier ou volume hors du SAE doit inclure :</p> <ul style="list-style-type: none"> <li>• (pour les séries) tous les dossiers et documents de la série ;</li> <li>• (pour les dossiers) tous les volumes et sous-dossiers du dossier ;</li> <li>• tous les documents de ces dossiers, sous-dossiers ou volumes ;</li> <li>• tout ou partie des métadonnées correspondantes ;</li> <li>• tout ou partie de l'historique des événements correspondant.</li> </ul> <p><i>Même si le SAE est en mesure d'exporter toutes les métadonnées et tout l'historique, cela n'est pas toujours demandé par le système cible.</i></p>	P
5.3.6	<p>Si le SAE exporte ou transfère un document avec ses métadonnées, il doit gérer explicitement les métadonnées implicites.</p> <p><i>Autrement dit, toutes les métadonnées visant une série, un dossier, sous-dossier, volume ou document doivent apparaître explicitement, même si elles ont été conservées de manière implicite. Voir les exemples en 9.3.</i></p>	P
5.3.7	<p>Lors d'un export ou d'un transfert, le SAE doit pouvoir effectuer une des deux opérations suivantes :</p> <ul style="list-style-type: none"> <li>• exporter ou transférer avec les documents les règles de conservation/destruction correspondantes, de sorte que ces règles puissent continuer à s'appliquer dans le système cible ;</li> <li>• imprimer un ou plusieurs rapports montrant les règles de conservation/destruction à appliquer à chaque jeu de documents, avec leurs caractéristiques.</li> </ul>	P
5.3.8	<p>Lors d'un export ou d'un transfert, le SAE doit pouvoir effectuer une des deux opérations suivantes :</p> <ul style="list-style-type: none"> <li>• exporter ou transférer avec les contrôles d'accès correspondants, de sorte que ces contrôles puissent continuer à s'appliquer dans le système cible ;</li> <li>• imprimer un ou plusieurs rapports montrant les contrôles d'accès à appliquer à chaque jeu de documents, avec leurs caractéristiques.</li> </ul>	P

Réf	Exigence	Test
5.3.9	<p>Le SAE doit être capable de transférer ou d'exporter un dossier ou le contenu d'une série en une seule opération, afin que :</p> <ul style="list-style-type: none"> <li>le contenu et la structure des documents électroniques ne soient pas modifiés ;</li> <li>tous les composants d'un document électronique (le cas échéant) soient exportés comme une seule unité ;</li> <li>tous les liens entre le document, ses métadonnées et l'historique des événements soient préservés ;</li> <li>tous les liens entre les séries, dossiers, sous-dossiers, volumes et documents soient préservés et puissent être réactivés dans le système cible.</li> </ul>	P
5.3.10	<p>En cas d'export de dossiers et/ou de volumes et/ou de sous-dossiers, s'il s'y trouve des pointeurs vers des documents classés dans d'autres dossiers (voir 3.4.24), le SAE doit exporter la totalité du document et pas seulement le pointeur.</p> <p><i>Le but est de s'assurer qu'il n'y aura pas de difficultés de résolution de pointeur entre le système source et le système cible.</i></p>	O
5.3.11	<p>Le SAE doit être capable de transférer ou d'exporter des documents dans leur format de capture.</p>	O
5.3.12	<p>Le SAE doit être capable de transférer ou d'exporter des documents dans le format dans lequel ils ont été <a href="#">convertis</a>.</p>	O
5.3.13	<p>Le SAE doit pouvoir convertir les documents transférés ou exportés dans le ou le format de transfert indiqué.</p> <p><i>Par exemple, un format XML approuvé ou un format ouvert.</i></p> <p><i>Cette exigence vise les durées de conservation longues où les documents doivent être automatiquement convertis dans des formats approuvés pour la conservation à long terme, après un laps de temps donné, sans affecter l'intégrité ni l'authenticité des documents.</i></p>	P
5.3.14	<p>Le SAE doit conserver tous les groupes, les documents et les autres informations transférées, au moins jusqu'à ce que le succès du transfert ait été confirmé.</p> <p><i>Il s'agit d'une mesure conservatoire, afin que les documents ne soient pas détruits avant que le destinataire ait confirmé que le transfert s'était bien passé.</i></p> <p><i>Voir 9.2.30 et 9.2.31 pour les exigences relatives aux rapports d'incident de transfert.</i></p>	O
5.3.15	<p>Le SAE doit détruire les groupes, documents et autres informations transférées à réception de la confirmation de la réussite du transfert, à l'exception des métadonnées conservées comme <a href="#">témoins</a>.</p>	O

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
	<i>Voir 5.3.19.</i>	
<b>5.3.16</b>	<p>Le SAE doit être capable d'exporter la totalité du contenu d'une série du plan de classement en une seule opération, de sorte que :</p> <ul style="list-style-type: none"> <li>• la position relative de chaque dossier dans le plan de classement soit préservée afin qu'on puisse reconstituer la structure du dossier ;</li> <li>• les métadonnées nécessaires à la reconstitution de la série dans son entier soient préservées et transférées avec les contenus de la série.</li> </ul>	P
<b>5.3.17</b>	Le SAE devrait fournir la possibilité d'ajouter des métadonnées utilisateurs aux dossiers électroniques sélectionnés pour un transfert vers les archives historiques.	O
<b>5.3.18</b>	<p>Le SAE doit s'assurer que toutes les conversions (copies) d'un document marqué « à détruire » sont détruites.</p> <p><i>Si un même document figure dans plusieurs dossiers (voir 3.4.24), ce document et ses conversions (copies) devraient être retirés du dossier au moment de la destruction de celui-ci mais ne devraient pas être supprimés tant que toutes les occurrences du document n'auront pas été détruites.</i></p>	O
<b>5.3.19</b>	<p>Le SAE doit fournir la possibilité de préserver des <a href="#">métadonnées-témoins</a> pour les entités détruites ou transférées :</p> <ul style="list-style-type: none"> <li>• séries ;</li> <li>• dossiers ;</li> <li>• sous-dossiers ;</li> <li>• volumes ;</li> <li>• documents classés directement dans une série.</li> </ul> <p><i>Dans certains cas, il est souhaitable de conserver une information sur les documents détruits. Ces métadonnées comprennent au moins la date de capture et toutes les métadonnées propres à identifier chaque document de manière unique avec ses liens dans le plan de classement. Voir le modèle de métadonnées de MoReq2.</i></p> <p><i>Ainsi il est toujours possible de savoir quels documents ont été archivés, leurs dates de destruction ou de sort final, sans avoir à conserver le détail des métadonnées des dossiers et des documents.</i></p>	O

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>5.3.20</b>	Les métadonnées-témoins (voir 5.3.19) doivent comporter au minimum : <ul style="list-style-type: none"><li>• la date de destruction ou de transfert ;</li><li>• le code de classement complet ;</li><li>• le titre ;</li><li>• la description ;</li><li>• l'utilisateur responsable de la destruction ou du transfert ;</li><li>• le motif de la destruction ou du transfert (référence à une règle de conservation/destruction ou raison saisie manuellement) ;</li><li>• toute référence attribuée par le système où les documents ont été transférés pour faciliter le repérage des documents transférés.</li></ul>	0
<b>5.3.21</b>	Le SAE doit permettre à un administrateur d'indiquer une liste de métadonnées complémentaires à ajouter aux métadonnées-témoins.	0
<b>5.3.22</b>	Le SAE doit pouvoir exporter les métadonnées-témoins lors de l'export des documents.  <i>Le but est de permettre la migration entre SAE.</i>	0
<b>5.3.23</b>	Le SAE doit permettre d'exporter une même information plusieurs fois.	0
<b>5.3.24</b>	Lorsque le SAE exporte ou transfère des informations, il devrait pouvoir produire à la demande un rapport énumérant les documents exportés ou transférés selon leur niveau de sécurité.	0

## 6. Capture et déclaration des documents

### Généralités

Ce chapitre expose les exigences relatives au processus de capture des documents dans un SAE. La première section (6.1) traite du processus de capture standard. La section suivante (6.2) traite de l'[import par lots](#) de documents d'autres systèmes, suivie par une section dédiée à la messagerie électronique car le sujet est important (6.3). La section 6.4 concerne les types de documents et la section 6.5 traite de l'intégration avec les systèmes de numérisation et d'imagerie.

### Terminologie

Le sens du mot « capture » est celui du langage courant, placé dans le contexte de la société et des technologies de l'information. Dans ce contexte, « capturer » l'information signifie la mettre en sécurité dans un système informatique. Ce sens est compatible avec la définition archivistique de « capture » comme « action d'enregistrer ou de sauvegarder une instance donnée d'un objet [numérique](#) » extraite de la base de données terminologique du projet InterPares 2<sup>1</sup>.

Il s'ensuit qu'un SAE peut capturer toutes sortes d'informations : les documents à archiver proprement dits, les métadonnées et parfois de simples documents de travail.

Le fait qu'un SAE puisse (parfois) capturer des documents de travail aussi bien que des documents archivables suggère que le terme « capture » n'est peut-être pas assez précis, car capturer un document pour l'archivage implique un processus plus complexe que la capture d'un simple document de travail. L'archivage suppose notamment le classement, l'[enregistrement](#) et la fixation des données qui ne sont pas nécessaires pour la capture d'un simple document. On dit parfois « déclarer » à l'archivage au lieu de « capturer ». Toutefois, « déclarer » peut se dire pour un document créé hors du SAE aussi bien que pour un document de travail déjà capturé dans le SAE.

Ce défaut de précision ne devrait pas avoir d'incidence sur la clarté de MoReq2.

Le glossaire de la section 13.1 donne des définitions plus complètes.

---

<sup>1</sup> [http://www.interpares.org/ip2/ip2\\_terminology\\_db.cf.m](http://www.interpares.org/ip2/ip2_terminology_db.cf.m)

## 6.1 CAPTURE

---

Les [documents électroniques](#) créés ou reçus dans le cadre des processus métier viennent aussi bien de l'interne que de l'externe. Ils sont de formats variés, produits par des auteurs différents et sont reçus soit comme de simples pièces soit inclus dans des dossiers avec d'autres composants (voir le glossaire pour la définition de « composant » dans le contexte de MoReq2).

Certains documents archivables sont créés en interne par les processus métier. D'autres sont reçus via divers canaux de communication : messagerie électronique, fax, courrier postal (scanné ou non), de la main à la main, à des fréquences et avec des volumes variables. La prise en compte de ces besoins variés requiert un système de capture des documents souple avec des contrôles pertinents.

Réf	Exigence	Test
6.1.1	<p>Le processus de capture du SAE doit, par ses contrôles et ses fonctionnalités, permettre aux utilisateurs de :</p> <ul style="list-style-type: none"><li>• capturer les documents électroniques quels que soient le format, le codage ou les autres caractéristiques techniques, et sans altération de leur contenu ;</li><li>• s'assurer que les documents archivés sont rattachés au plan de classement ;</li><li>• s'assurer que les documents archivés sont rattachés à un ou plusieurs dossiers ou séries.</li></ul>	P

*« Format » est défini dans le glossaire. L'exigence est de pouvoir capturer n'importe quel format de fichier.*

Il n'est pas prévu de tester cette exigence de capture et il n'est pas exigé que le SAE fasse des restitutions (voir le glossaire) de tous les formats possibles. MoReq2 du reste ne donne pas de liste de tous les formats à capturer, dans la mesure où ceux-ci varient dans le temps et avec l'évolution des logiciels. Toutefois, il n'y a aucun doute que les types de document à archiver seront variés ; ce sera notamment les documents régulièrement utilisés dans les bureaux :

- sorties d'applications tels que les suites bureautiques ;
- message électronique (voir la section 6.3) ;
- audio ;
- bases de données ;
- formats PDF ;
- images numérisées ;
- vidéos ;
- pages web.

*Dans certains cas, le SAE peut aussi devoir capturer d'autres types de documents tels que :*

Réf	Exigence	Test
	<ul style="list-style-type: none"> <li>• blogs ;</li> <li>• fichiers compressés (parfois appelés « archives » au sens informatique du terme) ;</li> <li>• agendas électroniques ;</li> <li>• formulaires électroniques ;</li> <li>• données de SIG (système d'information géographique) ;</li> <li>• informations provenant d'autres applications tels que comptable, paie, DAO (dessin assisté par ordinateur) ;</li> <li>• système de messagerie instantanée ;</li> <li>• documents multimédia ;</li> <li>• transactions réalisées via Internet ;</li> <li>• documents comportant des liens vers d'autres documents archivables ;</li> <li>• code source de logiciel et documentation de projet ;</li> <li>• données structurées (transaction EDI par exemple) ;</li> <li>• webcasts ;</li> <li>• wikis.</li> </ul> <p><i>Ces listes ne sont pas exhaustives.</i></p>	
6.1.2	<p>Le SAE ne doit imposer aucune limite au nombre de documents à archiver dans une série, un dossier, sous-dossier ou volume, ni au nombre total de documents stockés dans le SAE.</p> <p><i>De gros volumes de documents archivés tendront à rendre le système difficile à utiliser, et ce n'est en général pas conseillé. Cette exigence vise les situations où les gros volumes sont inévitables comme dans les environnements transactionnels.</i></p>	P
6.1.3	<p>En cas de capture d'un document formé de plusieurs composants (voir le glossaire), le SAE devra capturer tous les composants.</p>	P
6.1.4	<p>En cas de capture d'un document électronique de plus d'un composant, le SAE doit permettre de gérer le document comme une seule entité, en maintenant les liens entre les composants et en maintenant l'intégrité de la structure du document archivé.</p> <p><i>Exemples de documents composites :</i></p> <ul style="list-style-type: none"> <li>• les pages web avec des graphiques embarqués ;</li> <li>• un document bureautique texte avec un lien vers un tableau.</li> </ul> <p><i>Il peut arriver que les liens entre les composants ne fonctionnent pas s'ils sont simplement copiés dans l'entrepôt du SAE. Ainsi, de nombreuses pages web comportent des liens vers des graphiques ou d'autres objets avec des adresses (URL) extérieures à l'entrepôt ; et les tableaux liés contiennent en général des liens externes à l'entrepôt (noms de fichiers du système d'exploitation). Voir exigence suivante.</i></p>	P

Réf	Exigence	Test
6.1.5	<p>En cas de capture d'un document électronique de plus d'un composant, le SAE devrait modifier le document, si nécessaire, afin de préserver la possibilité de restitution. Autrement dit, le SAE pourra changer les références internes (liens) de certains composants.</p> <p><i>Cette exigence ne s'applique qu'aux seuls formats définis pour le SAE et non aux autres formats. Exemples :</i></p> <ul style="list-style-type: none"> <li>• pages HTML comportant des liens vers des graphiques ou autres objets ;</li> <li>• tableaux comportant des liens vers d'autres tableaux.</li> </ul> <p><i>Ceci est contraire au principe général de non modification du contenu des documents archivés, mais c'est inévitable pour des documents composites qui doivent être stockés dans leur format d'origine sans perdre leurs caractéristiques (liens, fidélité). Ces modifications sont acceptables dès lors qu'elles sont tracées dans l'historique de événements du SAE (voir exigence suivante). Une alternative consiste à convertir le document archivé dans un autre format (tel que <a href="#">PDF/A</a>) qui en préserve l'apparence ; voir exigence 11.7.8 ; d'un autre côté, si on évite de modifier les liens, on risque de les perdre.</i></p>	P
6.1.6	<p>Quand le SAE modifie les liens d'un document lors de la capture, le détail de l'opération doit être automatiquement tracé dans l'historique.</p>	O
6.1.7	<p>Le SAE doit automatiquement capturer le format de fichier (voir glossaire), y compris la <a href="#">version</a> de chaque composant capturé et stocker ces informations dans les métadonnées du composant ou du document.</p> <p><i>L'objectif est d'aider à la conservation et à l'accessibilité des documents numériques dans le temps. Voir section 11.7.</i></p> <p><i>Le format de fichier est parfois implicite dans l'extension du nom de fichier du composant (.htm ou .pdf) ; mais celle-ci est parfois ambiguë (.doc renvoie à plusieurs formats de fichiers hétérogènes). Par ailleurs, l'extension seule n'indique pas en général la version du format voire pas même le format. On peut s'en accommoder mais ce sera insuffisant en cas de conservation à long terme, ou si des précisions du type « espace couleur » sont requises.</i></p> <p><i>Les formats de fichier sont nombreux et sujets à de fréquentes évolutions. Il n'est donc pas réaliste d'attendre d'un SAE qu'il capture l'information dans tous les formats. Le SAE doit en revanche :</i></p> <ul style="list-style-type: none"> <li>• définir une liste des formats reconnus ;</li> <li>• se référer à un registre de formats officiel, si possible un registre consacré à la pérennisation de l'information numérique.</li> </ul> <p><i>Si ce n'est pas le cas, l'entreprise/organisation utilisatrice se contentera du panel des formats prédéfinis pour répondre à ses besoins de conservation.</i></p>	P

Réf	Exigence	Test
6.1.8	<p>Le processus de capture du SAE doit valider les valeurs des métadonnées saisies au moment de la capture, en conformité au minimum avec les règles du modèle de métadonnées de MoReq2.</p> <p><i>Voir aussi 6.1.34 dans cette section.</i></p>	0
6.1.9	<p>Le SAE devrait faciliter la validation des métadonnées à l'aide d'un algorithme de contrôle.</p> <p><i>Par exemple, les fichiers peuvent être identifiés par un numéro de carte de crédit à seize chiffres dont le dernier chiffre permet de vérifier les quinze autres avec un algorithme modulo 10.</i></p> <p><i>Pour ce faire, le recours à une API (interface de programmation) permettant d'intégrer les algorithmes des organisations, peut être considéré comme une solution acceptable.</i></p>	0
6.1.10	<p>Le SAE doit permettre aux utilisateurs de capturer un document électronique même en l'absence de l'application de production.</p> <p><i>Par exemple, un utilisateur peut recevoir en pièces jointes d'un courriel un plan de projet et un dessin en CAO/FAO. Si l'utilisateur n'a pas accès au plan de projet ou aux applications de CAO/FAO, il n'est pas en mesure de lire les documents. Malgré tout, il devrait pouvoir capturer ces pièces et les archiver dans le SAE. Le SAE pourrait fournir un visualiseur pour que l'utilisateur puisse lire ces documents. MoReq2 ne l'exige pas.</i></p>	0
6.1.11	<p>Le SAE doit pouvoir capturer les métadonnées des documents conformément au modèle de métadonnées de MoReq2.</p>	0
6.1.12	<p>Le SAE devrait pouvoir capturer automatiquement des valeurs de certains champs, définis par un administrateur pour tel ou tel document, et renseigner automatiquement les métadonnées avec ces valeurs comme l'indique le modèle de métadonnées de MoReq2.</p> <p><i>La fonctionnalité requise par cette exigence ne vaut que pour certains types d'objets électroniques, par exemple les lettres élaborées à partir d'un modèle et d'un traitement de texte.</i></p> <p><i>De nombreux documents, documents bureautiques, fichiers PDF ou autres, comportent des métadonnées définies par les utilisateurs. Il faudrait pouvoir configurer le SAE pour qu'il capture automatiquement ces valeurs et les conserve avec le document archivé.</i></p>	0
6.1.13	<p>Le SAE doit permettre la capture de toutes les métadonnées indiquées à la configuration du système, les relier aux documents électroniques archivés et maintenir ce lien en tout temps.</p>	0

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>6.1.14</b>	<p>Le SAE devrait permettre aux utilisateurs désireux d'archiver un document dont ils ne peuvent renseigner toutes les métadonnées obligatoires de le capturer et de le stocker temporairement dans le SAE.</p> <p><i>Autrement dit, le SAE devrait fournir un moyen de stocker des documents sans la totalité des métadonnées requises par le processus normal de capture. Ceci suppose un reporting et un contrôle des opérations ; mais il n'y a pas lieu d'archiver et de traiter ces documents dans une perspective d'export, de transfert, de conversion, etc. MoReq2 ne précise pas les modalités de l'opération.</i></p> <p>Seules les valeurs de métadonnées modifiables pourront varier ultérieurement ; les métadonnées fixes (ex : données d'envoi d'un courriel) ne doivent jamais changer.</p>	O
<b>6.1.15</b>	<p>Le SAE doit garantir que les valeurs de certaines métadonnées de documents peuvent être mises à jour par les utilisateurs ou administrateurs habilités, en accord avec les règles du chapitre 12.</p>	O
<b>6.1.16</b>	<p>Le SAE doit garantir que, au moment de la capture, tous les documents archivés sont rattachés à au moins une série, un dossier (ou au sous-dossier approprié), selon les besoins.</p>	O
<b>6.1.17</b>	<p>Le SAE devrait apporter une assistance automatique à la capture des documents électroniques par l'extraction automatique du maximum de métadonnées, pour le plus grand nombre possible de types de documents.</p> <p><i>Les raisons de cette exigence sont :</i></p> <ul style="list-style-type: none"><li>• <i>réduire le nombre de données saisies par les utilisateurs (l'expérience montre que bien souvent la saisie obligatoire des métadonnées conduit les utilisateurs à rejeter le système) ;</i></li><li>• <i>accroître l'exactitude des métadonnées.</i></li></ul> <p><i>Les métadonnées et les types de documents concernés, dépendront de l'environnement. Le modèle de métadonnées donne quelques explications.</i></p>	N

Réf	Exigence	Test
6.1.18	<p>Le SAE doit apporter une assistance automatique à la capture des documents entrants et sortants (ex : notes ou courriers avec telle présentation et tel format de fichier) par l'extraction automatique des métadonnées suivantes :</p> <ul style="list-style-type: none"> <li>• date du document (dans le corps du document) ;</li> <li>• destinataire(s)</li> <li>• destinataire(s) secondaire(s) ;</li> <li>• objet ;</li> <li>• auteur ;</li> <li>• référence (notre référence) ;</li> </ul> <p>dans la mesure où elles existent.</p> <p><i>MoReq2 ne précise pas le logiciel ou les formats pour les documents bureautiques ou la messagerie. L'extraction de métadonnées peut s'opérer en les localisant dans le document, à l'aide d'un gabarit qui les identifie et renseigne un formulaire vierge, ou par tout autre moyen.</i></p>	0
6.1.19	<p>Le SAE doit enregistrer la date et l'heure de la capture d'un document à la fois dans les métadonnées et dans l'historique.</p> <p><i>Si la date et l'heure sont partie intégrante de l'identifiant unique, et si elles peuvent en être extraites facilement, il n'est pas nécessaire de les stocker séparément.</i></p> <p><i>MoReq2 ne spécifie pas le niveau de précision de l'heure. La plupart des SAE enregistre l'heure à la seconde près au moins.</i></p> <p><i>Certains contextes réglementaires requièrent que l'horodatage soit effectué par un outil ou une autorité certifiés. Dans ce cas, l'exigence sera traitée dans le chapitre zéro.</i></p>	0
6.1.20	<p>Pour tout document capturé, le SAE doit pouvoir afficher à l'écran les métadonnées, y compris celles qui ont été indiquées au moment de la configuration.</p> <p><i>Les métadonnées indiquées au moment de la configuration renvoient à tout ou partie des métadonnées de la section correspondante du chapitre 12.</i></p>	0
6.1.21	<p>Le SAE doit s'assurer, pour chaque document capturé, de la présence de toutes les métadonnées obligatoires.</p>	0
6.1.22	<p>Pendant la capture d'un document, le SAE doit demander à l'utilisateur de saisir toute métadonnée nécessaire qui ne peut être capturée automatiquement.</p>	0
6.1.23	<p>Le SAE doit permettre l'attribution de plusieurs mots-clés (ou descripteurs) pour chaque série, dossier, sous-dossier ou document.</p> <p><i>MoReq2 n'exige pas de mot-clé pour les volumes.</i></p>	0

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>6.1.24</b>	Le SAE devrait permettre à un administrateur de définir si les mots-clés sont obligatoires ou optionnels, au moment de la configuration, pour chaque série, dossier ou sous-dossier.	0
<b>6.1.25</b>	Le SAE doit autoriser la création de plusieurs entités (série, dossier, etc.) portant la même combinaison de mots-clés.	0
<b>6.1.26</b>	Le SAE devrait permettre à un utilisateur de renseigner les mots-clés d'une nouvelle entité en les recopiant d'une autre entité, en une seule opération.	0
<b>6.1.27</b>	Le SAE devrait permettre à un utilisateur de saisir plusieurs identifiants de langues pour un document.	0
<b>6.1.28</b>	Le SAE doit donner la possibilité d'emprunter les valeurs des mots-clés ou d'autres métadonnées ou de les valider à l'aide de vocabulaires contrôlés (ou listes d'autorités).  <i>Par exemple, en utilisant un thésaurus. Voir aussi l'exigence 11.8.11.</i>	0
<b>6.1.29</b>	Le SAE doit permettre la saisie de descripteurs ou de métadonnées complémentaires, soit lors de la capture soit à une étape ultérieure du traitement.	0
<b>6.1.30</b>	Le SAE doit avertir l'utilisateur qui s'apprête à capturer un objet ou à renommer un objet avec un titre qui existe déjà au sein de la même entité.  <i>Voir aussi l'exigence 11.8.6.</i>	0
<b>6.1.31</b>	Le SAE doit pouvoir restreindre le droit de corriger le titre d'un document électronique archivé à un administrateur ou un utilisateur autorisé.  <i>Cette possibilité est laissée à l'appréciation de l'entreprise/organisation.</i>	0
<b>6.1.32</b>	Si un utilisateur capture un document qui possède plusieurs versions, le SAE doit lui permettre de : <ul style="list-style-type: none"> <li>• déclarer l'ensemble des versions comme un seul document ;</li> <li>• n'archiver qu'une seule des versions ;</li> <li>• déclarer séparément chaque version.</li> </ul>	0

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>6.1.33</b>	<p>Le SAE devrait fournir un module d'aide au rattachement des documents archivés au plan de classement en permettant l'une des actions suivantes :</p> <ul style="list-style-type: none"> <li>• Afficher seulement la partie du plan de classement accessible à l'utilisateur ou à son profil ;</li> <li>• proposer les séries ou dossiers les plus récemment utilisés par cet utilisateur ;</li> <li>• proposer les séries ou dossiers les plus fréquemment utilisés par cet utilisateur ;</li> <li>• proposer les séries ou dossiers repérés à partir des métadonnées du document (par exemple, les mots importants du titre ou l'objet du courriel) ;</li> <li>• proposer des dossiers ou des séries repérés à partir du contenu du document.</li> </ul>	P
<b>6.1.34</b>	<p>Le SAE devrait permettre que plusieurs utilisateurs interviennent dans le processus de capture d'un document.</p> <p><i>Le SAE devrait permettre de répartir le processus de capture entre les utilisateurs ; typiquement : un utilisateur saisit certaines métadonnées puis fait suivre le document électronique à un autre utilisateur qui saisit la suite des métadonnées et classe le document.</i></p>	O
<b>6.1.35</b>	<p>Le SAE devrait fournir les fonctionnalités d'un workflow simple pour faciliter la traçabilité de la vérification et de l'approbation d'un document avant sa capture : enregistrement des décisions prises, par qui et pour quel motif.</p> <p><i>A noter qu'il s'agit là d'un workflow basique, délibérément plus léger que le workflow complet décrit au chapitre 10.</i></p>	O
<b>6.1.36</b>	<p>Le SAE devrait fournir une interface de programmation pour recevoir et capturer en temps réel des documents ou transactions issus d'une autre application ou système.</p> <p><i>Comme précisé au point 1.4, les fonctionnalités d'archivage électronique peuvent être incluses dans un système plus large. Le SAE devrait alors recevoir des documents en provenance d'un autre système, par exemple une application métier du type « gestion de la relation client » (CRM) ou une application dédiée via une interface de programmation (API) pour permettre au SAE de capturer des documents individuellement.</i></p>	N
<b>6.1.37</b>	<p>Le SAE devrait si possible émettre une alerte quand un utilisateur tente de capturer un courriel qui a déjà été archivé dans le même dossier ou dans la même série (cas du rattachement direct à une série).</p> <p><i>MoReq2 ne précise pas comment ce courriel est repéré mais l'identifiant Internet devrait suffire.</i></p> <p><i>Il y a cependant des cas où ceci ne sera pas possible, par exemple si le courriel a été capturé dans un dossier auquel l'utilisateur n'a pas accès.</i></p>	O

Réf	Exigence	Test
6.1.38	Le SAE devrait si possible émettre une alerte quand un utilisateur tente de capturer un document (autre que le courriel évoqué en 6.1.37) qui a le même contenu qu'un autre document déjà enregistré dans le même dossier ou dans la même série (cas du rattachement direct à une série).	O
6.1.39	Le SAE devrait si possible émettre une alerte quand un utilisateur tente de capturer un document (autre que le courriel évoqué en 6.1.37) qui a les mêmes métadonnées d'identification qu'un autre document déjà enregistré dans le même dossier ou dans la même série (cas du rattachement direct à une série).  <i>Les métadonnées d'identification sont :</i> <ul style="list-style-type: none"> <li>• <i>titre ;</i></li> <li>• <i>date ;</i></li> <li>• <i>auteur ;</i></li> <li>• <i>destinataire.</i></li> </ul>	O
6.1.40	Le cas échéant, le SAE devrait pouvoir produire une alerte si quelqu'un tente de capturer un document dont le caractère incomplet ou incohérent risque de compromettre ultérieurement la fiabilité.  <i>Par exemple, un bon de commande sans signature électronique valide ou une facture d'un fournisseur non identifié.</i>	N
6.1.41	Le SAE doit permettre à un administrateur (et non aux utilisateurs) d'ajouter un document à un volume qui est clos, dès lors que la date du document n'est pas postérieure à la date de clôture. Dans ce cas : <ul style="list-style-type: none"> <li>• le SAE doit demander à un administrateur de saisir le motif de cette opération exceptionnelle dans les métadonnées du document et du volume ;</li> <li>• le SAE doit automatiquement enregistrer l'opération dans l'historique.</li> </ul> <p>Cette action ne doit pas mettre à jour la métadonnée « date de clôture ».</p> <p><i>Cette fonctionnalité doit permettre de corriger une erreur d'utilisateur, par exemple la clôture involontaire d'un volume. C'est pourquoi, il est important que la raison de cette action soit bien mentionnée.</i></p> <p><i>MoReq2 ne préjuge pas de la manière de procéder. Ce peut être une réouverture temporaire du volume clos ou une autre façon.</i></p>	O

## 6.2 IMPORT PAR LOTS

---

Les documents peuvent être archivés par lots dans le SAE de plusieurs façons. Par exemple :

- transfert par lot en provenance d'un système de GED compatible ;
- transfert par lot en provenance d'un SAE compatible ;

- fichier de données unique, compatible, contenant une série de documents homogènes (ex : factures du jour) ;
- en provenance d'un système de numérisation compatible ;
- documents issus des répertoires du système d'exploitation.

Le SAE doit pouvoir les recevoir ; il doit comporter les fonctionnalités de gestion du processus de capture et conserver le contenu et la structure des documents importés.

Au cours d'un import par lots, le SAE doit capturer les mêmes informations que lors d'un processus de capture normal - à savoir les documents et leurs métadonnées. Il doit également classer les documents - avec, le cas échéant, une extension du plan de classement (voir 3.1.12) - et si possible capturer les données d'historique. Enfin, l'import par lots doit permettre la gestion des exceptions et des erreurs.

Au moment où nous écrivons, le développement d'un schéma XML pour MoReq2 est prévu. Ce schéma a pour but de mettre en œuvre le modèle de métadonnées de MoReq2 ; il fournira un protocole optimal pour l'import de documents électroniques à partir d'un SAE conforme à MoReq2.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>6.2.1</b>	<p>Quand un schéma XML pour MoReq2 aura été formellement publié, le SAE devra pouvoir effectuer un import par lots conforme à ce schéma.</p> <p><i>Voir aussi l'exigence 5.3.1 sur l'export de documents archivés. Prises ensemble, ces deux exigences traitent de l'interopérabilité des systèmes conformes à MoReq2.</i></p>	P
<b>6.2.2</b>	<p>Le SAE doit fournir la possibilité de capturer des documents de transaction issus d'autres systèmes, notamment :</p> <ul style="list-style-type: none"><li>• l'assistance à l'import de fichiers de transaction en batch ;</li><li>• la fourniture de règles modifiables pour personnaliser la capture automatique des documents ;</li><li>• la validation de l'intégrité des données.</li></ul> <p><i>MoReq2 ne précise pas les modalités de ces opérations.</i></p>	P
<b>6.2.3</b>	<p>Le SAE doit pouvoir capturer automatiquement les métadonnées d'un document pendant l'import par lots (en permettant la saisie manuelle des métadonnées manquantes ou incorrectes).</p>	P

Réf	Exigence	Test
6.2.4	<p>Quand le SAE capture des métadonnées pendant un import, il doit les valider avec les mêmes règles que pour la capture manuelle des documents. Si ce processus de validation met en évidence des erreurs (absence de métadonnées obligatoires, erreurs de format), il doit attirer l'attention de l'utilisateur qui effectue l'import, identifier systématiquement les métadonnées en cause et tracer les erreurs et les corrections dans l'historique.</p> <p><i>Idéalement, les documents importés auront des métadonnées correspondant au modèle de métadonnées. Sinon, les métadonnées risquent de ne pas être conformes. Plusieurs actions sont alors possibles ; MoReq2 n'en privilégie aucune. Ce sont notamment :</i></p> <ul style="list-style-type: none"> <li>• annulation de la totalité de l'import ;</li> <li>• annulation de l'import pour les documents dont les métadonnées ne sont pas conformes ;</li> <li>• l'utilisateur doit soit corriger les erreurs soit annuler l'import des séries affectées ;</li> <li>• les données importées forment un document temporaire incomplet (à rapprocher de l'exigence de partage du processus de capture entre utilisateurs, cf. 6.1.34).</li> </ul>	0
6.2.5	<p>Le SAE doit pouvoir importer l'historique des événements qui trace l'historique des documents importés.</p>	0
6.2.6	<p>Le SAE ne doit pas intégrer l'historique d'import à son propre historique des événements ; il doit le stocker séparément.</p> <p><i>L'historique d'import doit être conservé séparément pour éviter de déclencher un mécanisme qui conduirait un administrateur à modifier ou compromettre l'intégrité de l'historique principal. MoReq2 ne précise pas les modalités de cette opération ; on peut stocker l'historique d'import en tant que document à la suite des documents importés, ou comme une entité séparée identifiée comme historique d'import d'un autre système.</i></p>	0
6.2.7	<p>Le SAE doit fournir des fonctions de gestion des files d'attente.</p> <p><i>Les fonctions souhaitées sont notamment :</i></p> <ul style="list-style-type: none"> <li>• voir les files d'attente ;</li> <li>• suspendre une ou plusieurs files d'attente ;</li> <li>• redémarrer une ou plusieurs files d'attente ;</li> <li>• détruire une file d'attente.</li> </ul>	0
6.2.8	<p>Le SAE doit donner à un administrateur la possibilité (s'il le souhaite) de clore automatiquement une série, des dossiers ou des volumes après leur import.</p> <p><i>Par exemple, en cas de fusion d'entreprises/organisations, il peut être nécessaire de clore certaines branches de l'arborescence de classement pour éviter qu'on y ajoute d'autres documents.</i></p>	0

## 6.3 GESTION DES MESSAGES ELECTRONIQUES

---

### Définitions

L'expression « messagerie électronique » renvoie au mécanisme de transmission de messages entre « agents » (le mot « agent » est employé ici dans un sens technique ; la compréhension de MoReq2 ne nécessite pas plus de détail).

Le protocole standard utilisé pour la messagerie électronique est défini par les documents RFC2821 et RFC2822 du Network Working Group (voir annexe 7). MoReq2 se base sur RFC2821/RFC2822 pour sa définition de « message électronique ».

L'expression « message électronique » renvoie à un document qui contient toutes les données d'une transmission électronique unitaire. Toutefois, bien que RFC2822 définisse la syntaxe pour la transmission des messages, aucune norme ne définit les formats de données à utiliser pour les messages qui doivent être capturés.

En d'autres termes, même si les applications de messageries des différents fournisseurs peuvent échanger librement des messages (en respectant les protocoles définis dans RFC2821/RFC2822), on ne peut être sûr, quand on capture un message dans une application donnée qu'un autre logiciel de messagerie pourra le relire. Chaque fournisseur de solution de messagerie utilise son ou ses format(s) propriétaires pour la capture des messages. Il s'ensuit qu'on ne peut garantir l'exactitude d'une extraction automatique des métadonnées à partir des messages.

### Usages et problématiques

La messagerie électronique est utilisée pour envoyer des documents (les messages eux-mêmes et/ou les pièces jointes) entre entreprises/organisations ou en interne. Les caractéristiques des logiciels de messagerie (notamment le défaut de normalisation pour les formats évoqués ci-dessus), combinées aux pratiques des utilisateurs, font que l'archivage au sens du « records management » peut être difficile à appliquer à la messagerie. Les entreprises/organisations doivent être en mesure de renforcer les procédures et les contrôles afin de :

- capturer la totalité des messages entrants ou sortants avec leurs pièces jointes ;

et/ou :

- capturer les messages et les pièces jointes en fonction de règles prédéfinies ;

et/ou :

- fournir aux utilisateurs la possibilité de capturer une sélection de messages et de pièces jointes.

Dans certains pays, la propriété juridique des courriels manque de clarté, et la capture automatique des messages dans un SAE peut s'avérer inappropriée. Dans ce cas, on ne prendra en compte lors de la configuration que les deux dernières options.

Par ailleurs, la messagerie électronique est devenue le moyen de communication par défaut de nombreuses entreprises/organisations et joue un rôle majeur pour les autres. Souvent, les courriels sont éphémères. C'est à chaque structure de choisir l'alternative qui représente le meilleur compromis eu égard à sa situation :

- la première option conduit à la capture de tous les messages, qu'ils soient éphémères ou qu'ils constituent des documents probants à archiver ;
- la deuxième option repose sur une configuration réussie de règles et de filtres adaptés ;
- la troisième option nécessite une évaluation de la pertinence et de l'importance des messages par les utilisateurs, avec le risque que tous n'agissent pas de manière fiable.

MoReq2 autorise les trois approches pour un SAE. Les procédures et les contrôles de gestion dépassent le cadre de MoReq2.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>6.3.1</b>	Quand un courriel est capturé, le SAE doit par défaut le capturer dans un format qui en conserve l'en-tête.	0
<b>6.3.2</b>	<p>Le SAE doit favoriser l'intégration de la capture des courriels, de sorte que la capture puisse être effectuée par un utilisateur à partir de l'application de messagerie, sans avoir besoin d'ouvrir le SAE.</p> <p><i>Cette intégration est essentielle pour l'efficacité d'un SAE. Ainsi, un utilisateur devrait pouvoir faire un « glisser-coller » de l'application cliente vers le SAE ; choisir la fonction « capture » depuis l'application cliente ; ou bien l'application de messagerie devrait signaler les courriels déjà capturés dans le SAE. Le point fort de cette exigence est que l'utilisateur ne doit pas avoir à ouvrir le SAE pour capturer les courriels.</i></p> <p><i>MoReq2 permet en outre (mais n'exige pas) la capture des courriels par d'autres voies, moins intégrées.</i></p>	0
<b>6.3.3</b>	<p>Il doit être possible de configurer le SAE dès le départ pour déclencher une des opérations suivantes lorsqu'un utilisateur envoie un courriel :</p> <ul style="list-style-type: none"> <li>• capture automatique du message ;</li> <li>• vérification de l'opportunité de la capture au regard des règles prédéfinies ;</li> <li>• notification automatique à l'utilisateur avec option de capture ou non ;</li> <li>• aucune action (c'est à l'utilisateur que revient d'initier ou non la capture).</li> </ul> <p><i>Quelle que soit la formule retenue, on peut accepter que le SAE demande à l'utilisateur de classer les documents manuellement et de saisir quelques métadonnées.</i></p>	0

Réf	Exigence	Test
6.3.4	<p>Il doit être possible de configurer le SAE dès le départ pour déclencher une des opérations suivantes lorsqu'un utilisateur reçoit un courriel :</p> <ul style="list-style-type: none"><li>• capture automatique du message (sauf s'il a déjà été capturé) ;</li><li>• vérification de l'opportunité de la capture au regard des règles prédéfinies ;</li><li>• si le courriel n'a pas déjà été capturé, notification automatique à l'utilisateur avec option de capture ou non ;</li><li>• aucune action (c'est à l'utilisateur que revient d'initier ou non la capture).</li></ul> <p><i>Quelle que soit la formule retenue, on peut accepter que le SAE demande à l'utilisateur de classer les documents manuellement et de saisir quelques métadonnées.</i></p>	O
6.3.5	<p>Le SAE doit fournir un module d'aide à la capture et à l'archivage des messages entrants et sortants, avec ou sans pièces jointes, avec extraction automatique des métadonnées suivantes :</p> <ul style="list-style-type: none"><li>• date d'envoi du courrier (voire heure) ;</li><li>• destinataire ;</li><li>• destinataires secondaires ;</li><li>• objet ;</li><li>• expéditeur ;</li><li>• signature électronique embarquée ;</li><li>• autorité de certification ;</li></ul> <p>dans la mesure où elles existent.</p> <p><i>Cette exigence demande la capture de « l'expéditeur » du message, lequel n'est pas toujours la même personne que l'auteur, par exemple quand une assistante envoie un message au nom de son directeur. Le terme « expéditeur » est ici un compromis délibéré, la capture automatique du nom d'auteur n'étant pas fiable. Les entreprises/organisations devraient étudier l'opportunité d'un manuel de procédures pour la correction des métadonnées d'auteur.</i></p> <p><i>L'annexe 9 donne des explications pour l'interprétation des métadonnées de courriel.</i></p>	P
6.3.6	<p>Les utilisateurs devraient pouvoir capturer un courriel et l'archiver dans un sous-dossier, un dossier ou une série en le faisant glisser de l'application cliente (techniquement un Agent) vers un sous-dossier, un dossier ou une série donnée du SAE.</p> <p><i>Le sous-dossier, le dossier ou la série peuvent être présentés dans une fenêtre de l'application de messagerie ou dans une fenêtre séparée.</i></p>	O

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>6.3.7</b>	<p>Le SAE doit permettre à un utilisateur de choisir entre plusieurs modes de capture du courriel et de ses pièces jointes :</p> <ul style="list-style-type: none"> <li>• le message seul, sans les pièces jointes ;</li> <li>• le message avec ses pièces jointes, comme un document unique constitué de plusieurs composants ;</li> <li>• les pièces jointes archivées séparément, comme autant de documents individuels.</li> </ul> <p><i>Ceci s'applique aux courriels envoyés aussi bien que reçus.</i></p> <p><i>La dernière de ces trois options signifie que la ou les pièces jointes sont archivées sans le contexte du message qui les a transmis.</i></p>	0
<b>6.3.8</b>	<p>Lorsqu'un message et ses pièces jointes sont capturés au même moment mais séparément, le SAE devrait automatiquement créer des liens entre les documents qui en résultent.</p> <p><i>Le SAE devrait permettre à un utilisateur de naviguer entre ces liens de sorte qu'il puisse voir chacune des pièces jointes à partir du message et le message à partir de n'importe laquelle des pièces jointes.</i></p>	0
<b>6.3.9</b>	<p>Si une pièce jointe est capturée et archivée séparément, le SAE doit exiger que les métadonnées correspondantes soient capturées et/ou saisies en même temps.</p>	0
<b>6.3.10</b>	<p>Lors de la capture d'un courriel, le SAE doit par défaut renseigner la métadonnée de titre avec l'objet du message.</p> <p><i>L'annexe 9 donne des explications pour l'interprétation des métadonnées de courriel.</i></p>	0
<b>6.3.11</b>	<p>Le SAE doit permettre à un utilisateur qui capture et archive un courriel d'en modifier le titre.</p> <p><i>Ceci a pour but de permettre aux utilisateurs de corriger les titres inappropriés, de les développer ou de les rendre plus explicites.</i></p> <p><i>Le titre du message est distinct de son objet ; ce dernier reste un élément du message, quel que soit le contenu du titre.</i></p>	0
<b>6.3.12</b>	<p>Si un utilisateur capture une notification de réception (le cas échéant) pour un message qui a été capturé, le SAE devrait pouvoir créer automatiquement un lien entre les deux.</p> <p><i>Les notifications de réception sont aussi bien des notifications de non distribution que des accusés de réception. Le SAE devrait permettre à un utilisateur de naviguer entre ces liens de sorte qu'il puisse voir ces notifications à partir du message et le message à partir de n'importe laquelle des notifications.</i></p>	0
<b>6.3.13</b>	<p>Le SAE doit permettre la capture automatique des métadonnées d'un message et de ses pièces jointes en référence au modèle de métadonnées de MoReq2.</p>	0

Réf	Exigence	Test
6.3.14	<p>Le SAE doit permettre que les métadonnées « date d'envoi » et « date de réception » soient saisies manuellement.</p> <p><i>Ceci vise les cas où les dates qui figurent dans le message ne correspondent pas à la réalité (voir une explication des cas de figure dans l'introduction de la section). On peut accepter qu'une option de configuration bloque cette fonction.</i></p>	0
6.3.15	<p>Un utilisateur doit pouvoir capturer dans le SAE, en une seule opération, une sélection manuelle de plusieurs courriels comme :</p> <ul style="list-style-type: none"> <li>• un document unique ;</li> </ul> <p>ou</p> <ul style="list-style-type: none"> <li>• une série de documents (un document par courriel) ;</li> </ul> <p>selon son choix.</p>	0
6.3.16	<p>Le SAE devrait pouvoir identifier automatiquement et capturer tous les messages liés à un message donné indiqué par l'utilisateur, en une seule opération, comme :</p> <ul style="list-style-type: none"> <li>• un document unique ;</li> </ul> <p>ou</p> <ul style="list-style-type: none"> <li>• une série de documents (un document par courriel) ;</li> </ul> <p>au choix de l'utilisateur.</p> <p><i>La section 3.6.4 du RFC2822 « Champs d'identification » décrit l'utilisation des champs d'en-tête SMTP (« référence » et « répondre à »), en lien avec le champ « identifiant du message », pour identifier les messages liés, ce qu'on appelle parfois « fil de discussion ».</i></p>	0
6.3.17	<p>Le SAE doit permettre à un utilisateur qui capture un courriel dans un format propriétaire de le sauvegarder en plusieurs formats, y compris ouverts.</p> <p><i>Le SAE aurait avantage à utiliser des critères de conservation basés sur les règles de conservation/destruction. Les contenus de message à durée de conservation courte pourraient être stockés dans un format propriétaire mais les messages à durée de conservation longue pourraient être sauvegardés dans un format ouvert.</i></p>	0
6.3.18	<p>Lorsque les adresses capturées dans l'en-tête apparaissent dans les métadonnées du message archivé, le SAE doit s'efforcer de capturer le nom de la personne détentrice de la boîte de messagerie (s'il existe) aussi bien que l'adresse proprement dite ; par exemple « Jean Durand » plutôt que « jdd97@xyz.int ».</p>	0

## 6.4 TYPES DE DOCUMENTS ARCHIVES

---

On entend par « types de documents archivés » les caractéristiques du document qui ne sont pas décrites (et ne sauraient l'être) dans le plan de classement. Ce sont notamment :

- les métadonnées correspondantes ;
- les exigences de conservation ;
- les contrôles d'accès ;
- la nature de la pièce (ex. : contrat, CV, rapport disciplinaire).

Le type d'un document archivé correspond habituellement à la nature de la pièce archivée.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
6.4.1	Le SAE doit aider à définir et à gérer les types de documents.	0
6.4.2	Tout document archivé dans le SAE doit avoir son type de document.	0
6.4.3	Le SAE doit réserver à un administrateur la définition et la gestion des types de documents.	0
6.4.4	Le SAE doit permettre à un administrateur de réserver la création de certains types de documents à certains groupes d'utilisateurs, sur la base des besoins métier.	0
6.4.5	Le SAE doit permettre à un administrateur de définir un type de document par défaut, utilisable par tous les utilisateurs qui capturent des documents.	0

## 6.5 NUMERISATION ET TRAITEMENT DE L'IMAGE

---

Dans un projet de SAE, il est souvent nécessaire de prendre en compte les [documents physiques](#) archivés sous forme papier ou microforme.

La problématique est double :

- le besoin de consulter les documents archivés sous forme papier ou microforme en référence aux documents électroniques ;
- les documents que l'entreprise/organisation continue de créer et de recevoir sous forme papier mais dont elle souhaite disposer sous forme électronique dans le SAE.

Cette section traite de la numérisation des documents papier et microforme en vue de leur capture et de leur archivage dans le SAE. Plusieurs des exigences qui suivent concernent le détail du processus de numérisation.

La numérisation peut s'effectuer de différentes façons :

- centralisée ;
- locale ou par un groupe de travail ;

- externalisée ou sous-traitée ;  
ou solution mixtes, brièvement décrites ci-après.

La numérisation centralisée est la plus adaptée pour les gros volumes, notamment si on utilise des scanners rapides conçus pour les imports par lots, en liaison avec des opérateurs spécialisés.

La numérisation locale ou par un groupe de travail, proche des utilisateurs, convient à de petits volumes d'activité, là où l'opérateur doit avoir une connaissance du métier, ou en cas de localisation éclatée des équipes. On utilise alors des scanners lents à faible capacité ; il s'agit parfois d'outils multifonctions.

Le choix d'externaliser ou de sous-traiter la numérisation tient à diverses raisons liées à la maîtrise des coûts :

- en cas d'un fort volume à numériser en une seule opération ;
- quand les ressources nécessaires en personnel ne sont pas disponibles de suite en interne ;
- quand les équipements nécessaires ne sont pas disponibles de suite en interne ;
- quand la numérisation et/ou le stockage sont indépendants du site.

La suite de cette section présente les exigences à prendre en compte en cas de solution de numérisation intégrée au SAE. Ces exigences ne s'appliquent que si les moyens de numérisation sont partie intégrante du SAE, bien que nombre d'entre elles puissent être également utiles en cas d'externalisation de la numérisation.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>6.5.1</b>	Le SAE doit être capable d'intégrer au moins une solution de numérisation.  <i>La solution de numérisation fournit une interface avec le scanner et permet à l'opérateur de numérisation d'effectuer divers processus tels que la rotation ou le gommage des taches.</i>	0
<b>6.5.2</b>	La solution de scan du SAE doit permettre le scan en noir et blanc et en couleur.  <i>De nombreuses applications n'ont pas besoin de la couleur.</i>	0
<b>6.5.3</b>	L'outil de scan du SAE doit être capable de sauvegarder des images dans les formats standards, soit (liste non exhaustive) : <ul style="list-style-type: none"> <li>• TIFF (voir les spécifications TIFF 6.0)</li> <li>• JPEG (voir ISO 15444, en cas de numérisation en couleur) ;</li> <li>• PDF/A (voir ISO 19005).</li> </ul>	0
<b>6.5.4</b>	L'outil de scan du SAE doit être capable de conserver des images en différentes résolutions.  <i>Dans l'idéal, l'outil de scan devrait fournir un menu d'option, à paramétrer en fonction des différents types de documents à capturer.</i>	0
<b>6.5.5</b>	L'outil de scan du SAE doit être capable de conserver des images en couleur ou en niveaux de gris et en différentes résolutions.	0

Réf	Exigence	Test
6.5.6	<p>L'outil de scan du SAE doit être capable de gérer les formats de papier standards, soit (liste non exhaustive) :</p> <ul style="list-style-type: none"> <li>• A4</li> <li>• A3</li> </ul> <p><i>Voir ISO 216 pour la définition de A4 et A3.</i></p>	0
6.5.7	<p>L'outil de scan du SAE devrait posséder une fonction de reconnaissance optique de caractères (OCR).</p> <p><i>L'OCR restituée du texte à partir d'une image scannée. Certains types d'OCR sont parfois appelés ICR (reconnaissance intelligente de caractères). Pour simplifier, MoReq2 appelle les deux OCR.</i></p>	0
6.5.8	<p>Lorsque le SAE inclut une fonction d'OCR, il devrait pouvoir gérer l'image scannée et le texte qui en résulte comme un seul document.</p> <p><i>Autrement dit, le texte ocrisé devrait être considéré comme une métadonnée du document archivé plutôt que comme un document à part entière.</i></p> <p><i>MoReq2 n'exige pas que l'utilisateur puisse voir le texte ocrisé, dès lors qu'il peut y faire une recherche en texte intégral (voir exigence suivante).</i></p>	0
6.5.9	<p>Lorsque le SAE inclut une fonction d'OCR, il devrait permettre la recherche en texte intégral sur le texte ocrisé.</p>	0
6.5.10	<p>L'outil de scan du SAE devrait pouvoir reconnaître et capturer des documents individuellement dans un processus de numérisation de masse.</p> <p><i>MoReq2 ne précise pas comment procéder. Les solutions courantes reposent sur une reconnaissance des codes patch, des pages patch, de codes barres ou des pages blanches.</i></p>	0
6.5.11	<p>L'outil de scan du SAE doit être capable de diriger automatiquement les images scannées vers une file d'attente.</p> <p><i>Par exemple, pour l'indexation ou l'assurance qualité.</i></p>	0
6.5.12	<p>Le SAE devrait inclure une facilité de contrôle des images scannées.</p> <p><i>Ceci sous-entend de pouvoir accepter ou rejeter les images ; et, en cas de rejet, de recommencer l'opération.</i></p> <p><i>Le contrôle peut être effectué par un opérateur de numérisation, par un responsable qualité, ou par tout utilisateur qui effectue cette vérification dans le cours de son travail.</i></p>	0
6.5.13	<p>L'outil de scan du SAE devrait permettre à un administrateur de fixer un seuil pour le contenu de l'image de sorte que, sous ce seuil, l'image soit rejetée comme une page blanche.</p>	0

Réf	Exigence	Test
6.5.14	L'outil de scan du SAE devrait pouvoir stocker les données de paramétrage du scan (ex : recto-verso, résolution, contraste, luminosité) pour différents types de document.	0
6.5.15	Le SAE devrait permettre aux utilisateurs d'annoter les images.  <i>Cette fonction peut servir à noter les problèmes particuliers lors de la numérisation, ou pour des annotations (cf. les notes manuscrites sur les documentations papier).</i>	0
6.5.16	Si le SAE permet aux utilisateurs d'annoter les images retenues pour l'archivage, il doit interdire la modification ou la suppression de ces annotations.  <i>Ceci ne s'applique qu'aux documents à archiver, non aux autres images. Le but est d'éviter que les documents archivés ne soient (ou ne semblent) modifiés.</i>	0
6.5.17	Si le SAE permet aux utilisateurs d'annoter les images retenues pour l'archivage, il doit enregistrer l'identité de l'auteur de chaque annotation avec la date et l'heure, de façon inaltérable.  <i>Ceci ne s'applique qu'aux documents à archiver, non aux autres images. Le but est de garantir que ces annotations sont pertinentes et tracées.</i>	0
6.5.18	L'outil de scan du SAE devrait enregistrer le détail de chaque opération de numérisation, à savoir : <ul style="list-style-type: none"> <li>• nom de l'utilisateur (login) ;</li> <li>• identifiant du poste de travail ;</li> <li>• date et durée ;</li> <li>• identifiant de la session ;</li> <li>• identifiant(s) de batch ;</li> <li>• nombre de documents (si possible) ;</li> <li>• nombre d'images numérisées ;</li> <li>• nombre d'images après le retrait des pages blanches (si cette opération est automatique).</li> </ul>	0
6.5.19	L'outil de scan du SAE devrait pouvoir capturer automatiquement les métadonnées pertinentes à partir de formulaires à zones.  <i>Un formulaire à zones comporte certaines parties où le logiciel de numérisation peut localiser les données à numériser. L'information extérieure à ces zones n'est pas scannée, ce qui réduit la taille de l'image et les besoins de stockage ou de bande passante.</i>	0

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>6.5.20</b>	Quand l'outil de scan du SAE inclut une capture automatique des métadonnées, il devrait pouvoir en déduire automatiquement où classer le document.  <i>Cette fonction est particulièrement utile pour la gestion de dossiers sériels : ces dossiers papier comportent souvent des zones d'identification avec des données suffisantes pour classer le document archivé - voir section 10.5.</i>	0
<b>6.5.21</b>	Le SAE devrait pouvoir réaliser des imports par lots d'images scannées avec leur métadonnées.  <i>Voir section 6.2 pour plus de détails sur l'import par lots.</i>	0
<b>6.5.22</b>	Le SAE devrait pouvoir afficher les vignettes des images scannées pour faciliter la navigation et la recherche.	0
<b>6.5.23</b>	Le SAE doit permettre aux utilisateurs de capturer des images pour les archiver.	0

# 7. identification

Ce chapitre regroupe les exigences pour l'identification des entités (séries, dossiers, sous-dossiers, volumes et documents) au sein d'un plan de classement. Les exigences de la section 7.1 concernent les codes de classement et celles de la section 7.2 les identifiants système.

Toutes les entités stockées dans l'entrepôt d'un SAE (séries, dossiers, sous-dossiers, volumes, documents, etc.) requièrent des identifiants dans le but de :

- permettre au logiciel de traiter les entités ;
- permettre aux utilisateurs de repérer les entités, de s'y référer et de les utiliser.

MoReq2 décrit les identifiants à l'aide de la terminologie suivante :

- un identifiant exigé pour le fonctionnement du logiciel est appelé « identifiant système ». Il peut aussi être utilisé par les utilisateurs dans certains cas ;
- un identifiant hiérarchique affecté aux entités du plan de classement hiérarchique et destiné aux utilisateurs est appelé « code de classement » ;
- d'autres identifiants sont nommés en fonction des besoins, par exemple : « identifiant de conservation/destruction ».

La différence entre les identifiants système et les codes de classement est illustrée par les trois schémas ci-après. Ces schémas sont également évoqués à la fin du chapitre.

La figure 7.1 montre une portion d'un plan de classement fictif mais réaliste. On y voit quelques séries avec leur libellé (comme demandé en 0).

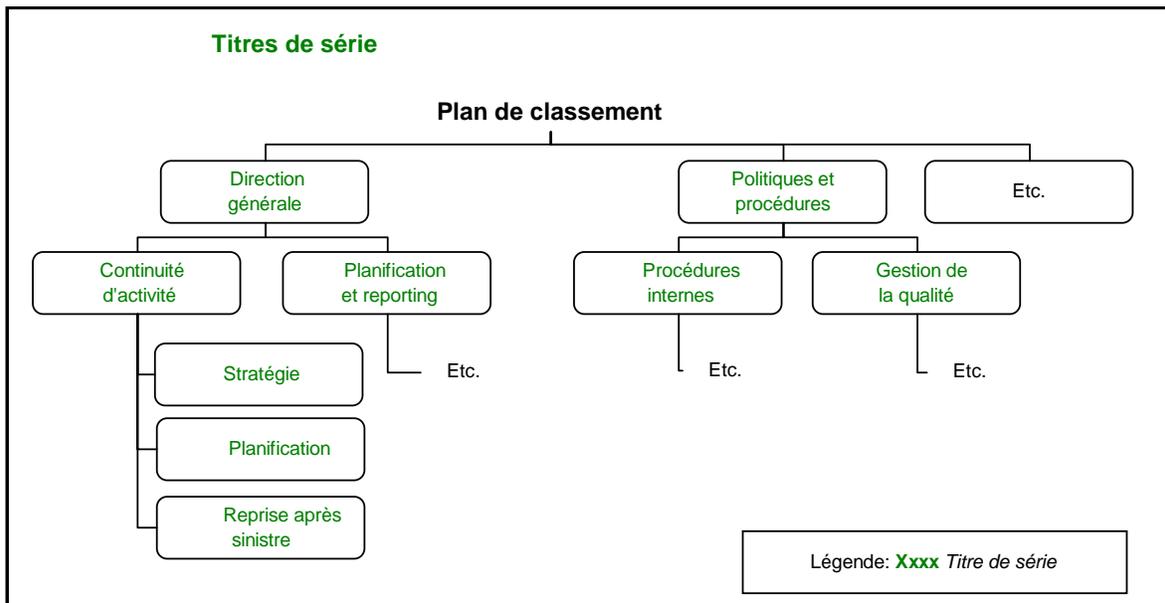


Figure 7.1

Chaque série reçoit un identifiant système, comme le montre la figure 7.2.

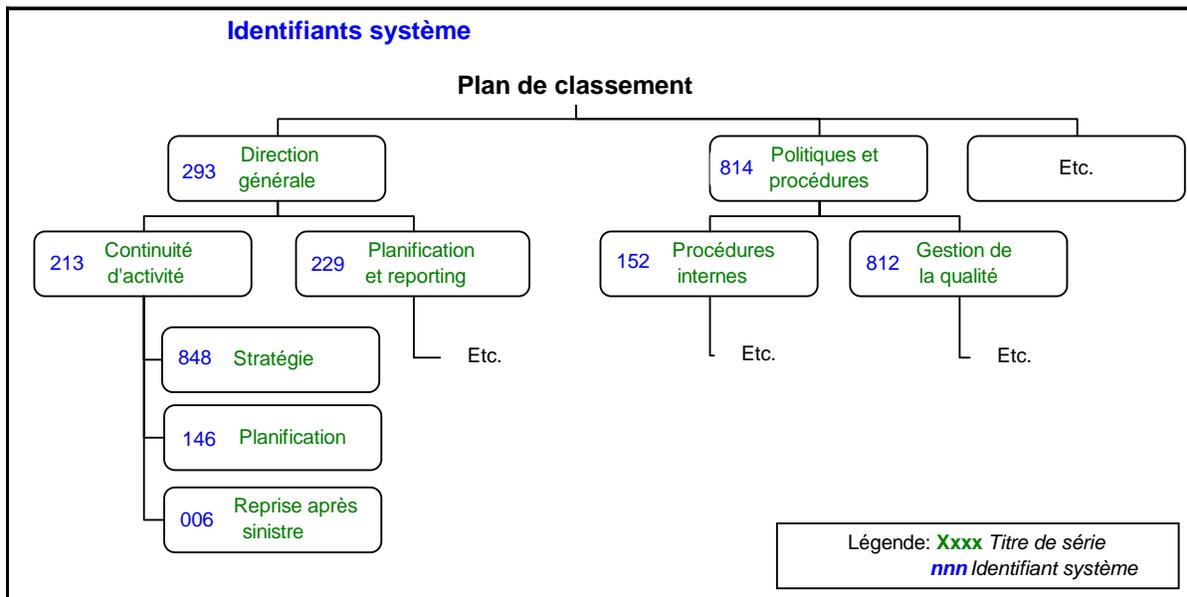


Figure 7.2

A noter que les identifiants système sont ici courts et simples, à titre d'exemple. Dans la réalité, ils seront plus longs, avec une structure plus complexe. Pour donner un exemple, un identifiant système basé sur l'algorithme « Identifiant Global Unique » pourrait être 0c7220e3-5646-44c4-82b0-67832c1efa1c.

Les séries reçoivent également un code de classement qui peut revêtir plusieurs formes comme indiqué plus loin ; la figure 7.3 en donne un exemple.

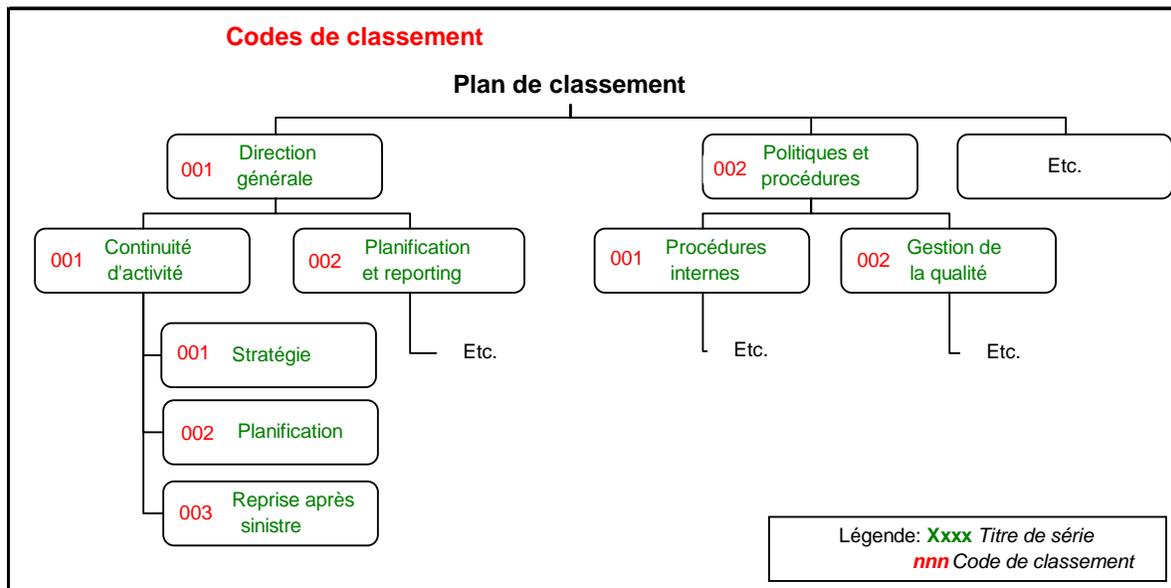


Figure 7.3

Ici aussi, les codes de classement sont relativement simples, pour la démonstration.

Le code de classement de chaque série peut être combiné avec les codes de classement des séries supérieures pour constituer un « code de classement complet ». Dans cet exemple, le code de classement complet pour Reprise après sinistre est 001-001-003. Il est construit ainsi :

- en tête, le code de classement de la série la plus élevée dans la hiérarchie (001 étant le code de classement de la série *Direction générale*)
- on ajoute le code de classement de la série immédiatement en dessous dans la hiérarchie (001 étant le code de classement de la série *Continuité d'activité*), ce qui donne 001-001 ;
- on répète l'étape précédente jusqu'à la série la plus proche (ce qui n'est pas le cas dans cet exemple très simple) ;
- on ajoute le code de classement de la série (003), code de classement de la série *Reprise après sinistre*, ce qui donne le code de classement complet 001-001-003.

Les documents et leurs composants reçoivent aussi des codes de classement afin d'être dotés d'un identifiant unique.

Le degré d'unicité requis dépend des usages prévus. Les identifiants système doivent en général être uniques au sein d'un SAE ou d'un nœud de réseau (c'est un minimum) et si possible pour tout le réseau. Les codes de classement complets doivent être uniques au sein du plan de classement puisqu'ils sont construits en descendant la hiérarchie, chaque code de classement complet étant unique à partir d'un nœud de la hiérarchie (ex : série ou sous-dossier).

Lorsque l'unicité est requise pour l'ensemble du réseau, il est souhaitable que les identifiants système s'inspirent d'une norme reconnue qui garantit l'unicité globale (l'unicité à travers tous les systèmes et en tout temps). Ceci est également souhaitable pour les applications indépendantes ou non reliées au réseau, pour laisser la possibilité d'une extension ultérieure ou en cas de fusion/acquisition d'activités. Plusieurs normes existent dans ce domaine mais aucune ne s'est imposée ; MoReq2 ne recommande donc pas de norme particulière sur ce sujet.

## 7.1 CODES DE CLASSEMENT

---

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
7.1.1	Lorsqu'une nouvelle occurrence d'une des entités suivantes est créée ou capturée par le SAE, il doit lui attribuer un code de classement : <ul style="list-style-type: none"> <li>• série ;</li> <li>• dossier ;</li> <li>• sous-dossier ;</li> <li>• volume ;</li> <li>• document ;</li> <li>• composant.</li> </ul>	O
7.1.2	Le SAE doit s'assurer que les codes de classement complets sont uniques au sein du plan de classement hiérarchique.	P

Réf	Exigence	Test
7.1.3	Le SAE doit s'assurer que tous les codes de classement et tous les codes de classement complets conservent leur degré d'unicité, même en cas de déplacement (voir l'exigence 3.4.1).	0
7.1.4	Le SAE doit permettre de stocker les codes de classement parmi les métadonnées des entités correspondantes.	0
7.1.5	Le SAE devrait permettre à un administrateur de définir les formats des codes de classement et des codes de classement complets au moment de la configuration. Il devrait permettre de définir les caractéristiques des codes de classement, pour chaque niveau de la hiérarchie, à savoir : <ul style="list-style-type: none"> <li>• numérique, alphabétique ou alpha-numérique ;</li> <li>• présence ou absence de zéros initiaux ;</li> <li>• longueur minimum (en cas de zéros initiaux) ;</li> <li>• valeur de départ ;</li> <li>• incrémentation.</li> </ul>	0
7.1.6	Les codes de classement complets doivent résulter d'une concaténation des codes de classement, avec des séparateurs.	0
7.1.7	Le SAE devrait permettre de choisir les séparateurs des codes de classement complets au minimum parmi : <ul style="list-style-type: none"> <li>• * * (espace)</li> <li>• *-* (tiret)</li> <li>• */* (slash avant)</li> <li>• *.* (point).</li> </ul> <p><i>Ainsi, le code de classement 001-001-003 (voir l'exemple ci-dessus) pourrait se présenter sous diverses formes, en fonction des choix opérés pour les zéros initiaux et les séparateurs, par exemple :</i></p> <ul style="list-style-type: none"> <li>• 1 001 003 ;</li> <li>• 001-001-003 ;</li> <li>• 1/1/3 ;</li> <li>• 001.001.003.</li> </ul> <p><i>Noter que l'exigence 3.2.7 permet l'utilisation de préfixes globaux et d'extensions, ce qui pourrait donner :</i></p> <ul style="list-style-type: none"> <li>• direction/1/1/3 ;</li> <li>• 001.001.3.pt.</li> </ul>	0



## 7.2 IDENTIFIANTS SYSTEME

Réf	Exigence	Test
7.2.1	<p>Lorsqu'une nouvelle occurrence d'une des entités suivantes est créée dans le SAE, il doit lui attribuer un identifiant système :</p> <ul style="list-style-type: none"> <li>• plan de classement ;</li> <li>• série ;</li> <li>• dossier ;</li> <li>• sous-dossier ;</li> <li>• volume ;</li> <li>• document ;</li> <li>• <a href="#">extrait</a> ;</li> <li>• règle de conservation/destruction</li> <li>• pièce.</li> </ul>	O
7.2.2	<p>Le SAE doit garantir que tous les identifiants système sont uniques au sein du plan de classement hiérarchique et au sein du système d'archivage.</p> <p><i>A noter que cette exigence vise l'ensemble des sites géographiques dans le cas où un plan de classement distribué a été mis en œuvre, et l'ensemble des plans de classement si plusieurs coexistent.</i></p>	N
7.2.3	<p>Le SAE doit être capable de stocker les identifiants système parmi les métadonnées des entités correspondantes.</p>	O
7.2.4	<p>Le SAE devrait attribuer des identifiants système globalement uniques.</p> <p><i>« Globalement uniques » signifie que les identifiants système sont attribués à l'aide d'un algorithme qui garantit qu'aucun autre identifiant système ne peut avoir la même valeur, quels que soient la date et l'outil de production.</i></p> <p><i>Ceci est souhaitable pour permettre les reconfigurations, nécessités notamment par les réorganisations, les fusions/acquisitions, etc. Si les entités ne sont pas dotées d'un identifiant système globalement unique, les reconfigurations peuvent poser de sérieuses difficultés.</i></p>	N
7.2.5	<p>Le SAE doit utiliser un algorithme UUID (défini par ISO/IEC 9834-8 et par ITU-Y Rec.X667) pour générer les identifiants système globalement uniques.</p> <p><i>Cet algorithme, couramment appelé GUID (Globally Unique ID) peut être utilisé pour garantir l'unicité.</i></p> <p><i>On peut utiliser d'autres méthodes que la génération d'identifiants uniques, par exemple le système DOI® (Digital Object Identifier), l'URN (Uniform Resource Name) ou l'ARK (Archival Resource Key).</i></p>	P
7.2.6	<p>Le SAE ne doit en aucun cas demander aux utilisateurs de saisir ou de se servir des identifiants système pour une autre fonction du système.</p>	P

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
	<i>Cette exigence vient de ce que les identifiants globalement uniques sont très longs et peu « conviviaux ». Toutefois, on peut admettre qu'un utilisateur soit autorisé à utiliser des identifiants système s'il le demande.</i>	

## 8. Recherche, repérage et restitution

Ce chapitre énumère les exigences pour la recherche et la localisation (section 8.1). Les exigences liées à la restitution sont divisées en trois sections : affichage (section 8.2), impression (section 8.3) et restitution des documents archivés non imprimables (section 8.4).

La capacité pour l'utilisateur à retrouver les dossiers et les documents fait partie intégrante d'un SAE, c'est-à-dire la recherche des documents, même en l'absence d'indications précises, et leur restitution. La restitution consiste à produire une représentation à l'écran (affichage ou impression) ; il peut aussi s'agir de produire du son ou de la vidéo (voir le glossaire).

L'accès aux dossiers et aux documents, puis leur visualisation exigent toute une série de fonctions de recherche, localisation et restitution afin de répondre aux besoins des différents types d'utilisateurs. Même si l'on peut penser que certaines fonctions dépassent le domaine de l'archivage et du records management, les fonctionnalités requises sont décrites ici en partant du principe qu'un SAE sans possibilités de recherche est d'un intérêt limité.

Toutes les caractéristiques et fonctionnalités de ce chapitre sont soumises aux contrôles d'accès décrits plus haut, y compris les contrôles de sécurité. Le SAE ne doit jamais fournir une information à un utilisateur qui n'est pas autorisé à la recevoir. Pour éviter la complexité, ce point est énoncé ici et n'est pas répété pour chaque exigence.

### 8.1 RECHERCHE ET REPERAGE

La recherche est le processus d'identification des documents et dossiers au travers de paramètres prédéfinis dans le but de localiser les documents, séries, dossiers, sous-dossiers, volumes et/ou métadonnées, d'y accéder et de les consulter.

Les outils de recherche et de navigation du SAE servent à localiser les métadonnées, les séries, les dossiers, sous-dossiers, volumes ou documents, ce qui exige un ensemble de techniques de recherche au service des utilisateurs, depuis l'utilisateur confirmé jusqu'à l'utilisateur occasionnel moins familier de l'informatique.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>8.1.1</b>	Une fonction de recherche d'un SAE ne doit en aucun cas révéler à un utilisateur une information (métadonnée ou contenu) que les contrôles d'accès et de sécurité (sections 4.1 et 10.13) lui interdiraient.	P

<b>Réf</b>	<b>Exigence</b>	<b>Test</b>
<b>8.1.2</b>	<p>Le SAE doit permettre à l'utilisateur de rechercher et de retrouver :</p> <ul style="list-style-type: none"> <li>• des documents ;</li> <li>• tout groupe de documents (série, dossier, sous-dossier, volume) ;</li> </ul> <p>et les métadonnées associées à n'importe quel niveau de classement.</p>	0
<b>8.1.3</b>	<p>Le SAE doit permettre à l'utilisateur de choisir toute combinaison de métadonnées comme terme de recherche.</p> <p><i>La recherche doit pouvoir se faire à partir de n'importe quelle métadonnée, par exemple le titre.</i></p>	0
<b>8.1.4</b>	<p>Le SAE doit permettre à l'utilisateur d'indiquer si la recherche vise à retrouver des documents ou un groupe spécifique de documents.</p>	0
<b>8.1.5</b>	<p>La fonction de recherche du SAE devrait se présenter de la même façon à l'utilisateur pour toutes les recherches indiquées en 8.1.2</p> <p><i>Autrement dit, l'utilisateur devrait voir les mêmes interfaces, fonctions et options, qu'il recherche des séries, des dossiers, des sous-dossiers, des volumes ou des documents (même si la présentation des résultats peut varier selon la nature de la recherche).</i></p>	0
<b>8.1.6</b>	<p>Le SAE doit permettre à l'utilisateur de faire des recherches sur les contenus.</p> <p><i>Ceci vise tous les documents qui sont par nature textuels, tels que courriels ainsi que (si le SAE comprend une fonction d'OCR) les documents convertis en texte par océrisation (voir l'exigence 6.5.7).</i></p>	0
<b>8.1.7</b>	<p>Le SAE doit permettre de faire des requêtes pour localiser un groupe de document dans le but de déclarer une entité ou comme étape d'un processus de déclaration.</p> <p><i>C'est une question de convivialité. Il s'agit de rendre la fonction recherche accessible à un utilisateur qui est en train de capturer un ou plusieurs documents ; celui-ci ne doit pas être contraint d'abandonner le processus de capture pour lancer une recherche.</i></p>	0
<b>8.1.8</b>	<p>Le SAE doit permettre à l'utilisateur d'utiliser toute combinaison de métadonnées et/ou de contenus textuels comme critères de recherche au cours d'une requête.</p> <p><i>Par exemple, une recherche pourra combiner un nom d'auteur avec tel passage d'un document.</i></p>	0
<b>8.1.9</b>	<p>Le SAE devrait fournir une fonction de recherche qui agit de manière intégrée et cohérente sur l'ensemble des contenus et des métadonnées.</p> <p><i>Cela signifie que l'interface devrait se comporter de la même façon pour les différentes recherches.</i></p>	0
<b>8.1.10</b>	<p>Le SAE doit afficher le nombre total de réponses à la recherche et afficher la liste des résultats (ou permettre à l'utilisateur d'en demander l'affichage).</p>	0

Réf	Exigence	Test
8.1.11	<p>Le SAE devrait permettre à l'utilisateur d'affiner (préciser) une recherche sans avoir à ressaisir les critères de recherche.</p> <p><i>Un utilisateur devrait par exemple pouvoir partir des résultats d'une première recherche pour en effectuer une autre sur cette base.</i></p>	0
8.1.12	<p>Le SAE doit permettre à un administrateur de configurer puis de modifier la liste des métadonnées de recherche par défaut, avec :</p> <ul style="list-style-type: none"> <li>• toute métadonnée de document, volume, sous-dossier, dossier ou série, et</li> <li>• éventuellement, du texte.</li> </ul> <p><i>Ceci renvoie à la fenêtre qui apparaît par défaut quand on lance une recherche ; elle comporte en général une suite de champs correspondant aux métadonnées les plus courantes (c'est-à-dire les métadonnées de recherche par défaut).</i></p>	0
8.1.13	<p>Le SAE doit fournir une fonction de recherche qui permet l'usage d'opérateurs booléens :</p> <ul style="list-style-type: none"> <li>• ET ;</li> <li>• OU ;</li> <li>• SEULEMENT ;</li> <li>• NE PAS ;</li> </ul> <p>et toute combinaison valable avec un nombre illimité de termes de recherche.</p>	P
8.1.14	<p>Le SAE doit permettre à l'utilisateur de rechercher des objets à partir des mots-clés, s'ils en ont.</p>	0
8.1.15	<p>Au cours d'une recherche avec mots-clés, le SAE doit permettre à l'utilisateur de choisir les mots-clés dans un vocabulaire contrôlé (ou liste d'autorité).</p> <p><i>A noter que, selon l'exigence 8.1.7, cela peut avoir lieu pendant le processus de capture ou pendant toute recherche.</i></p>	0
8.1.16	<p>Le SAE devrait inclure l'utilisation d'un thésaurus pour permettre la recherche par concepts.</p>	0
8.1.17	<p>Si le SAE inclut un thésaurus pour la recherche par concept, il devrait se conformer au moins à l'une de ces deux normes :</p> <ul style="list-style-type: none"> <li>• ISO 2788 ;</li> <li>• ISO 5964.</li> </ul> <p><i>Il s'agit de repérer des documents à l'aide de termes élargis, restreints ou approchant du contenu ou des métadonnées. Par exemple : « services ophtalmologiques » conduira à « services de santé », « test oculaire » ou « ophtalmologie ».</i></p> <p><i>La première norme vise un thésaurus monolingue et la seconde un thésaurus multilingue (voir 3.2.13 et 3.2.14).</i></p>	0

Réf	Exigence	Test
8.1.18	<p>Si un thésaurus conforme à ISO 2788 ou ISO 5964 est intégré dans le SAE, le SAE devrait permettre à l'utilisateur qui fait une recherche avec un mot-clé (ou une métadonnée liée au thésaurus) d'exploiter toutes les possibilités du thésaurus : termes élargis, restreints ou approchants et synonymes dans le cours normal du processus.</p> <p><i>Autrement dit, si un utilisateur cherche un dossier, il peut saisir un terme qui ne figure pas dans le vocabulaire contrôlé puis utiliser les fonctions du thésaurus pour trouver le mot approprié. Par exemple, « budget » est le terme approprié : l'utilisateur pourrait saisir « évaluations » et être guidé vers des termes plus larges tels que « budget » ; ou alors, l'utilisateur pourrait saisir « documents comptables » et se voir proposer une liste de termes proches dont « budget ».</i></p> <p><i>Il est souhaitable que l'utilisateur n'ait pas à abandonner l'interface de recherche pour utiliser le thésaurus et trouver les termes associés. Se reporter à l'introduction de la section 11.8 pour plus de détail sur l'expression « dans le cours normal du processus ».</i></p>	0
8.1.19	<p>Quand le SAE inclut l'utilisation d'un thésaurus, il doit permettre qu'il soit maintenu par un administrateur.</p> <p><i>Cette gestion est nécessaire en cas d'ajout de nouveaux mots ou de la terminologie spécifique aux métiers.</i></p>	0
8.1.20	<p>Le SAE doit restreindre aux administrateurs la possibilité de modifier les mots-clés d'un dossier.</p> <p><i>Cette opération doit rester exceptionnelle (corriger des erreurs de saisie, etc.). Une modification inopportune de mots-clés peut sérieusement compromettre l'accès aux documents, même si elle est tracée dans l'historique des événements, et est donc à éviter.</i></p>	0
8.1.21	<p>Le SAE devrait permettre les correspondances approximatives et la recherche approximative en avant, en arrière ou dans le corps des contenus et les métadonnées.</p> <p><i>Exemple :</i></p> <ul style="list-style-type: none"> <li>• le terme « proj » pourra repérer les documents contenant « projet », « projection » ou « PROJA » ;</li> <li>• le terme « psycho » pourra repérer les documents contenant « psychose », « psychotique » et « psychologues » ;</li> <li>• le terme « octet » collectera « gigaoctet » et « teraoctet » ;</li> <li>• le terme « pa ?e » pourra repérer les documents contenant « paie » ou « paye ».</li> </ul>	0
8.1.22	<p>Le SAE devrait fournir la recherche de proximité.</p> <p><i>Une recherche de proximité repère les mots séparés par un nombre maximum de mots, par exemple :</i></p> <ul style="list-style-type: none"> <li>• « international » et « organisation » séparés par un mot au maximum.</li> </ul>	0

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>8.1.23</b>	Le SAE doit permettre à l'utilisateur de limiter le champ de sa recherche à un groupe de documents indiqué au début de la recherche.	0
<b>8.1.24</b>	Le SAE doit pouvoir rechercher et repérer en une seule opération un dossier, un sous-dossier ou un volume électronique complet, avec ses subdivisions et ses métadonnées, et afficher la liste précise de toutes les entrées de ce groupe.  <i>C'est le cas si un utilisateur veut, par exemple, copier ou imprimer la totalité du contenu d'un dossier pour une réunion, pour travailler dessus.</i>	0
<b>8.1.25</b>	Le SAE doit se comporter de la même manière, que les objets recherchés soient stockés en ligne, en différé ou hors ligne, même si le mécanisme et la vitesse de restitution des objets électroniques peuvent varier.  <i>Cette exigence ne s'applique que lorsque le SAE gère également un stockage différé ou hors ligne.</i>	P
<b>8.1.26</b>	Le SAE devrait permettre à l'utilisateur de sauvegarder et de réutiliser ses termes de recherche.	0
<b>8.1.27</b>	Le SAE devrait permettre à un utilisateur de sauvegarder ses termes de recherche à destination d'autres utilisateurs.	0
<b>8.1.28</b>	Le SAE devrait permettre à l'utilisateur de spécifier des intervalles de temps pour sa requête (des dates ou des nombres de jours).	0
<b>8.1.29</b>	Le SAE devrait permettre l'utilisation comme termes de recherche d'intervalles de temps indiqués sous forme de dates (24 décembre 2008-5 janvier 2009) ou en langage naturel (« la semaine dernière », « ce mois-ci »), plus précisément les termes ci-après et/ou leurs équivalents dans d'autres langues : <ul style="list-style-type: none"> <li>• dernier ;</li> <li>• présent ;</li> <li>• prochain ;</li> <li>• semaine ;</li> <li>• mois ;</li> <li>• trimestre ;</li> <li>• année ;</li> <li>• noms des jours de la semaine ;</li> <li>• noms des mois.</li> </ul>	0
<b>8.1.30</b>	Le SAE devrait permettre à un utilisateur ou un administrateur de configurer l'affichage des résultats de recherche, notamment : <ul style="list-style-type: none"> <li>• sélection de l'ordre de présentation des résultats ;</li> <li>• indication du nombre de réponses affichées sur chaque page d'écran ;</li> <li>• fixation d'un nombre maximum de réponses pour une recherche ;</li> <li>• choix des métadonnées à afficher dans la liste des résultats.</li> </ul>	0

Réf	Exigence	Test
8.1.31	Le SAE devrait fournir un ordre logique, implicite ou explicite, de classement des résultats de recherche.	O
8.1.32	Quand les réponses incluent un extrait de document électronique ou un document dont il a été fait un extrait (cf. section 9.3), le SAE devrait relier les deux, de sorte que le repérage de l'un signale l'autre et y donne accès, sous réserve des droits d'accès, tout en distinguant bien leurs métadonnées respectives.	O
8.1.33	Le SAE devrait permettre la configuration d'un moteur de recherche différent du moteur initial.	N

*Une entreprise/organisation peut souhaiter implémenter un moteur de recherche autre que celui d'origine, pour une question de compatibilité ou pour une autre raison.*

## 8.2 RESTITUTION : AFFICHAGE DES DOCUMENTS

---

Un SAE peut contenir des documents de différents formats. L'utilisateur a besoin d'un outil de restitution générique qui facilite l'affichage de divers formats.

Réf	Exigence	Test
8.2.1	<p>Quand un utilisateur a atteint une fenêtre qui indique l'existence d'une série, d'un sous-dossier, sous-dossier, volume ou document, le SAE doit pouvoir restituer son contenu et/ou ses métadonnées en un seul clic de souris ou une seule commande clavier.</p> <p><i>Ceci est valable quelle que soit la façon dont l'utilisateur a atteint cette fenêtre : en navigant dans le plan de classement, par le biais d'une requête, en suivant un lien ou autre - en supposant que l'utilisateur a les droits.</i></p> <p><i>Exemple :</i></p> <ul style="list-style-type: none"> <li>• un utilisateur fait une recherche et obtient une liste de résultats de plusieurs documents ; pour chacun d'eux, le SAE doit pouvoir afficher le contenu par un simple clic de souris ou une commande clavier de l'utilisateur, et il doit restituer les métadonnées de la même façon ;</li> <li>• un utilisateur navigue dans le plan de classement jusqu'à une série contenant des dossiers ; le SAE doivent pouvoir afficher une liste de tous les dossiers de la série par un simple clic de souris ou une commande clavier de l'utilisateur, et il doit restituer les métadonnées de la même façon.</li> </ul> <p><i>Si le SAE stocke des documents dans un format propriétaire, on peut accepter que la restitution soit effectuée au travers d'une application externe au SAE.</i></p>	O

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>8.2.2</b>	Le SAE devrait pouvoir restituer les documents qui forment le résultat d'une recherche sans charger le logiciel associé.  <i>Une solution courante est d'intégrer au SAE un progiciel de visualisation. Cela est souvent souhaitable pour accélérer la vitesse de restitution.</i>	O
<b>8.2.3</b>	Le SAE devrait pouvoir restituer tous les types de documents électroniques définis par l'entreprise/organisation tout en préservant le contenu des documents (caractéristiques de présentation et de mise en page du progiciel d'origine, etc.), et en restituant en même temps tous les composants du document électronique.  <i>L'entreprise/organisation doit spécifier les logiciels et formats nécessaires, et dans certains cas les degrés de fidélité acceptés. Souvent (environnement bureautique notamment) l'exigence de fidélité est modérée ; en revanche, une exigence rigoureuse de fidélité peut être nécessaire pour des applications où l'interprétation du détail joue un rôle important, par exemple avec des images de rayon X en haute résolution.</i>	N

## 8.3 RESTITUTION : IMPRESSION

---

Cette section ne concerne que les documents et autres informations dont le contenu peut faire l'objet d'une impression compréhensible. Il ne s'applique donc pas aux fichiers audio et vidéo.

Le SAE doit fournir des facilités d'impression pour permettre aux utilisateurs d'obtenir des impressions des documents imprimables, de leurs métadonnées ou d'autres informations de gestion.

Dans toutes ces exigences, le mot « impression » renvoie aux fonctions normalement associées à la production de rapport : rapports multi-pages, numérotation des pages, en-têtes datés, utilisation d'une imprimante correctement configurée. L'envoi brut d'une image d'écran à une imprimante n'est en général pas suffisant pour répondre à ces exigences.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>8.3.1</b>	Le SAE doit pouvoir imprimer le contenu des documents avec les métadonnées demandées.	O
<b>8.3.2</b>	Le SAE doit permettre l'impression de tout ou partie des métadonnées d'une série, d'un dossier, sous-dossier, volume ou document.	O
<b>8.3.3</b>	Le SAE doit permettre d'imprimer en une seule opération tous les documents d'une série, d'un dossier, d'un sous-dossier ou d'un volume.	O
<b>8.3.4</b>	Le SAE doit permettre à l'utilisateur de définir un jeu de métadonnées (titre, auteur, date de création, etc.) et d'en imprimer la liste pour toute sélection de groupes de documents.	O

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>8.3.5</b>	<p>Le SAE devrait permettre à un administrateur de préciser au moment de la configuration que toutes les impressions de documents doivent comporter une sélection de métadonnées par défaut, soit : titre, numéro d'enregistrement, date, <a href="#">niveau de sécurité</a>.</p> <p><i>Ceci sera utile par exemple pour s'assurer que le niveau de sécurité d'un document est imprimé en même temps que lui, par mesure de sécurité.</i></p>	0
<b>8.3.6</b>	Le SAE devrait permettre à l'utilisateur, lors de l'impression, de corriger le jeu de métadonnées par défaut attaché à l'impression.	0
<b>8.3.7</b>	Le SAE doit permettre à l'utilisateur d'imprimer la liste des résultats d'une recherche (voir section 8.1).	0
<b>8.3.8</b>	<p>Le SAE doit permettre à un administrateur d'imprimer tout ou partie des paramètres de gestion.</p> <p><i>Exemple : la liste des utilisateurs avec tel niveau de sécurité, ou les utilisateurs de tel groupe d'utilisateurs.</i></p>	0
<b>8.3.9</b>	Le SAE doit permettre à un administrateur d'imprimer les règles de conservation/destruction.	0
<b>8.3.10</b>	Si un thésaurus est intégré (cf. 8.1.16), le SAE devrait permettre à un administrateur de l'imprimer.	0
<b>8.3.11</b>	<p>Le SAE doit pouvoir imprimer chacun des vocabulaires contrôlés (listes de tous les termes autorisés).</p> <p><i>Il peut suffire d'imprimer la liste à partir du logiciel de gestion du thésaurus s'il est intégré au SAE.</i></p>	0
<b>8.3.12</b>	Le SAE doit pouvoir exporter chacun des vocabulaires contrôlés (listes de tous les termes autorisés).	0
<b>8.3.13</b>	<p>Lorsque le vocabulaire contrôlé des mots-clés a la forme d'un thésaurus conforme à ISO 2788 ou ISO 5964, le SAE devrait pouvoir imprimer les entrées du thésaurus, montrant tous les termes et leurs relations.</p> <p><i>L'impression des thésaurus conformes à l'ISO doit respecter le guide pour la restitution joint à ISO 2788 et ISO 5964.</i></p> <p><i>Il peut suffire d'imprimer cette liste à partir d'un logiciel de gestion de thésaurus intégré au SAE.</i></p>	0
<b>8.3.14</b>	Le SAE doit permettre à un profil autorisé d'imprimer le plan de classement soit en totalité soit série par série.	0
<b>8.3.15</b>	<p>Un utilisateur qui imprime un plan de classement (cf. 8.3.14) devrait pouvoir préciser le contenu et le format de l'impression.</p> <p><i>Par exemple, l'utilisateur devrait pouvoir spécifier les métadonnées à imprimer et s'il souhaite une liste, une arborescence ou un graphique.</i></p>	P

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>8.3.16</b>	Le SAE doit permettre aux administrateurs d'imprimer une liste (appelée parfois répertoire) de tous les dossiers ou des dossiers rattachés à telle ou telle série (avec ses séries filles).	0
<b>8.3.17</b>	Un utilisateur qui imprime une liste de dossiers (cf. 8.3.16) devrait pouvoir spécifier l'ordre, le contenu et le format de la liste.  <i>Par exemple, l'utilisateur devrait pouvoir opérer un tri croissant ou décroissant des titres ou des codes, et si possible de n'importe quel attribut ; et il devrait pouvoir indiquer les métadonnées à imprimer.</i>	0
<b>8.3.18</b>	Le SAE doit permettre aux administrateurs d'imprimer tout ou partie de l'historique des événements (voir 4.2.1).	0
<b>8.3.19</b>	Le SAE doit pouvoir imprimer les formats définis par l'entreprise/organisation. L'impression doit : <ul style="list-style-type: none"><li>• conserver la mise en page du progiciel d'origine ;</li><li>• inclure toutes les composantes imprimables du document électronique.</li></ul> <i>L'entreprise/organisation doit définir les formats dont elle a besoin.</i>	0

## 8.4 RESTITUTION : AUTRES CAS

---

Cette section ne concerne que les documents et autres informations dont le contenu ne peut faire l'objet d'une impression compréhensible, tels que les fichiers audio et vidéo.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>8.4.1</b>	Le SAE doit comporter des fonctions de restitution et d'export vers des supports appropriés des documents non imprimables.  <i>Exemple : le son, la vidéo, des sites web, etc. L'entreprise/organisation devra préciser la nature de ces documents.</i>	P

## 9. Fonctions d'administration

Ce chapitre traite de la maintenance du système et des fonctions supports requises par un SAE.

Les exigences de ce chapitre concernent :

- l'administration générale (9.1) ;
- la fonction reporting (9.2) ;
- la modifications, la suppression et le masquage des documents archivés (9.3)

Certaines notions proches sont décrites au chapitre 4, à savoir :

- les autorisations d'accès (section 4.1) ;
- les sauvegardes et restaurations (section 4.3).

Ces fonctionnalités permettent aux administrateurs de gérer les évolutions des utilisateurs et les paramètres de fonctionnement du système. Le SAE doit fournir aux administrateurs la possibilité de gérer des événements tels que la maintenance de l'annuaire et surtout les autorisations accordées aux utilisateurs, groupes et profils. Le système doit aussi pouvoir contrôler les erreurs système.

Certaines de ces fonctions peuvent être fournies par un système de GED associé, un système de gestion de bases de données, un système d'exploitation ou d'autres applications.

### 9.1 ADMINISTRATION GENERALE

Cette section comprend les exigences de gestion des paramètres système, la gestion et la configuration du système et la gestion des utilisateurs.

Dans les grandes structures, ces tâches peuvent être attribuées à une fonction opérationnelle plutôt qu'à un responsable d'application. Mais dans des structures plus petites, on peut les confier à un administrateur.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>9.1.1</b>	Le SAE doit permettre aux administrateurs de retrouver, afficher et reconfigurer les paramètres système et les choix faits au moment de la configuration.  <i>Ces dispositions incluent notamment la configuration des droits d'accès ou les codes de classement.</i>	O
<b>9.1.2</b>	Le SAE doit permettre aux administrateurs : <ul style="list-style-type: none"> <li>• d'attribuer des fonctions aux utilisateurs et aux profils ;</li> <li>• d'attribuer un ou plusieurs utilisateurs à un profil.</li> </ul>	O
<b>9.1.3</b>	Le SAE doit gérer l'espace de stockage et demander aux administrateurs d'intervenir quand l'espace de stockage disponible est inférieur à ce qui a été défini lors de la configuration, ou par suite d'une autre erreur.	P

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
	<i>On peut accepter que cette notification aux administrateurs se fasse par le biais d'un logiciel de gestion séparé.</i>	
9.1.4	Si le stockage permet de mesurer les taux d'erreur, le SAE devrait contrôler les taux d'erreur sur les supports de stockage, et signaler aux administrateurs tout support ou infrastructure de stockage où ce taux dépasse le seuil défini au moment de la configuration ou plus tard.  <i>Ceci s'applique particulièrement aux supports optiques.</i>  <i>On peut accepter que cette notification aux administrateurs se fasse par le biais d'un logiciel de gestion séparé.</i>	N
9.1.5	Le SAE devrait permettre aux administrateurs de déplacer facilement des utilisateurs entre les groupes et les rôles.  <i>Il devrait notamment être possible de déplacer un utilisateur sans avoir à le supprimer du SAE et à ressaisir ses coordonnées.</i>	O

## 9.2 REPORTING

---

La souplesse du reporting est une caractéristique important du SAE. Il est indispensable que les administrateurs puissent piloter et gérer efficacement le système, afin de s'assurer qu'il est utilisé à bon escient.

Un SAE doit pouvoir produire tous les rapports de gestion, statistiques ou autres nécessaires aux administrateurs pour contrôler l'activité et l'état du système. Ce reporting s'applique à la totalité du système, y compris :

- le plan de classement ;
- les dossiers et les documents ;
- l'activité des utilisateurs ;
- les autorisations d'accès et la sécurité ;
- le sort final.

Le SAE doit produire un nombre de rapports statistiques types, paramétrables par les administrateurs ; il devrait être suffisamment souple pour produire des rapports à la demande.

Dans l'idéal, le SAE comportera un sous-système statistique souple. Il n'est pas pertinent de vouloir reproduire ici toutes les exigences d'un tel système ; la présente section se limite donc aux exigences principales. Le nombre et la complexité des rapports sera définie à partir des caractéristiques propres à l'entreprise/organisation : taille, complexité et changements affectant le plan de classement, volume et nature des documents archivés, nombre d'utilisateurs.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
------------	-----------------	-------------

Réf	Exigence	Test
9.2.1	Le SAE doit permettre aux administrateurs de produire des rapports périodiques (journaliers, hebdomadaires, mensuels, trimestriels) et de définir des rapports <i>ad hoc</i> .	0
9.2.2	Le SAE doit inclure des fonctions d'impression des rapports, d'affichage à l'écran et de stockage en ligne sous forme électronique.  <i>Comme à la section 8.3, le mot « impression » inclut les fonctions généralement associées à la production de rapports : rapports multi-pages, numérotation des pages, datation, en-tête et pied de page paramétrables, et usage de n'importe quelle imprimante. L'envoi d'une image d'écran à une imprimante n'est pas considéré comme suffisant dans ce cas.</i>	0
9.2.3	Un utilisateur qui visualise un rapport du SAE devrait pouvoir le capturer et l'archiver.  <i>Par exemple pour conserver de manière sécurisée les rapports attestant de l'intégrité des documents archivés.</i>	0
9.2.4	Le SAE devrait permettre que le laps de temps couvert par un rapport soit paramétré sous forme de dates (ex : 24/12/2008-5/1/2008) ou exprimée en langage naturel (voir 8.1.29).	0
9.2.5	Le SAE doit inclure des fonctions de tri et de choix des informations contenues dans le rapport.  <i>Par exemple, les utilisateurs devraient pouvoir définir sur quelles colonnes d'un rapport en forme de tableau se fera le tri des informations.</i>	0
9.2.6	Le SAE devrait inclure des fonctions de compilation ou de résumé des données des rapports.	0
9.2.7	Le SAE devrait inclure des fonctions graphiques.  <i>Par exemple, des courbes montrant l'évolution des statistiques dans le temps, ou des histogrammes.</i>	0
9.2.8	Le SAE doit permettre la sauvegarde et la réutilisation des requêtes statistiques.	0
9.2.9	Le SAE doit permettre l'export des rapports pour exploitation dans d'autres applications.  <i>Exemple : un utilisateur peut souhaiter travailler le contenu d'un rapport à l'aide d'un tableur. MoReq2 ne précise pas le(s) format(s) à utiliser pour ce type d'export.</i>	0

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>9.2.10</b>	<p>Le SAE doit pouvoir produire des rapports sur le nombre total et la localisation :</p> <ul style="list-style-type: none"> <li>• des dossiers, sous-dossiers et volumes ;</li> <li>• des documents triés par format et par version ;</li> <li>• des dossiers, sous-dossiers et volumes triés par droits d'accès et niveaux de sécurité ;</li> <li>• des dossiers, sous-dossiers et volumes électroniques triés par taille ;</li> <li>• des dossiers, sous-dossiers et volumes électroniques triés par localisation ;</li> <li>• des documents vitaux.</li> </ul>	P
<b>9.2.11</b>	<p>Le SAE doit pouvoir produire des rapports sur :</p> <ul style="list-style-type: none"> <li>• le pourcentage de documents capturés et archivés ;</li> <li>• le pourcentage de documents consultés ;</li> <li>• le pourcentage de création de nouvelles séries et dossiers.</li> </ul>	O
<b>9.2.12</b>	<p>Si l'option de GED décrite en 10.3 existe, le SAE doit pouvoir fournir des rapports sur :</p> <ul style="list-style-type: none"> <li>• le nombre total et la localisation des documents ;</li> <li>• le taux de capture/création des documents ;</li> <li>• le taux de repérage des documents.</li> </ul>	O
<b>9.2.13</b>	<p>Le SAE devrait permettre la production des rapports définis en 9.2.11 et 9.2.12 en combinant plusieurs critères :</p> <ul style="list-style-type: none"> <li>• tout le système ou telles ou telles séries ;</li> <li>• tels ou tels utilisateurs ou groupes d'utilisateurs ;</li> <li>• telle ou telle période.</li> </ul>	O
<b>9.2.14</b>	<p>Le SAE devrait permettre de produire des rapports sur les opérations effectuées par un utilisateur sur les dossiers et documents, par poste de travail (si cela est pertinent) ou par adresse réseau.</p>	P
<b>9.2.15</b>	<p>Le SAE devrait permettre, pour les rapports définis en 9.2.11, de préciser un intervalle plus court que sept jours.</p> <p><i>Par exemple, un graphe horaire montrant les pics et les creux d'activité à contrôler.</i></p>	O
<b>9.2.16</b>	<p>Le SAE doit pouvoir produire une liste des dossiers, sous-dossiers et volumes pour tout ou partie du plan de classement, dans l'ordre du plan de classement.</p>	O
<b>9.2.17</b>	<p>Le SAE doit pouvoir produire un rapport sur la part de l'espace de stockage système en cours d'utilisation ou disponible.</p>	O

Réf	Exigence	Test
9.2.18	<p>Le SAE doit permettre aux administrateurs d'effectuer des requêtes sur l'historique des événements. Ces rapports doivent porter au minimum sur une des entités suivantes :</p> <ul style="list-style-type: none"> <li>• série ;</li> <li>• dossier ;</li> <li>• sous-dossier ;</li> <li>• volume ;</li> <li>• document ;</li> <li>• utilisateur ;</li> <li>• laps de temps.</li> </ul>	0
9.2.19	<p>Le SAE devrait permettre aux administrateurs d'effectuer des requêtes dans l'historique et de produire des rapports sur :</p> <ul style="list-style-type: none"> <li>• les niveaux de sécurité ;</li> <li>• les groupes utilisateurs ;</li> <li>• d'autres métadonnées.</li> </ul>	0
9.2.20	<p>Le SAE doit pouvoir produire un rapport d'exécution du processus de destruction, avec la liste des séries, dossiers, sous-dossiers, volumes et documents détruits, et les anomalies.</p>	0
9.2.21	<p>Le SAE doit pouvoir produire un rapport d'exécution du processus d'export, avec la liste des séries, dossiers, sous-dossiers, volumes et documents exportés, et les anomalies.</p>	0
9.2.22	<p>Le SAE doit pouvoir fournir aux administrateurs un rapport sur les opérations de révision, mentionnant les actions en attente.</p>	0
9.2.23	<p>Le SAE devrait permettre aux administrateurs de restreindre l'accès des utilisateurs à certains rapports.</p>	0
9.2.24	<p>Le SAE doit pouvoir fournir aux administrateurs un rapport sur les tentatives d'accès indues ou autres violations des règles de sécurité.</p> <p><i>Cette exigence s'applique quand le SAE (et/ou le système d'exploitation) est configuré pour qu'un utilisateur puisse connaître l'existence d'un document même s'il n'a pas le droit d'y accéder. Si le SAE est configuré pour cacher aux utilisateurs l'existence des documents auxquels il n'a pas accès, ce point est sans objet.</i></p>	0
9.2.25	<p>Les administrateurs devraient pouvoir définir la fréquence des statistiques sur les règles de conservation/destruction, avec pointage des anomalies (sort final en attente, etc.).</p>	0
9.2.26	<p>Le SAE devrait fournir des rapports quantitatifs sur les volumes et les types de documents devant être révisés à une date donnée.</p>	0

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>9.2.27</b>	<p>Le SAE devrait comporter des outils d'analyse statistique pour aider un administrateur à gérer les règles de conservation/destruction, notamment la possibilité de :</p> <ul style="list-style-type: none"> <li>• lister toutes les règles de conservation/destruction, triées par motif ou date ;</li> <li>• lister toutes les entités dotées d'une règle de conservation/destruction spécifique ;</li> <li>• lister les règles de conservation/destruction qui s'appliquent à toutes les entités d'une même série ;</li> <li>• identifier, comparer et réviser les règles de conservation/destruction du plan de classement (avec leur contenu) ;</li> <li>• identifier les contradictions entre les règles de conservation/destruction dans l'ensemble du plan de classement.</li> </ul>	0
<b>9.2.28</b>	Le SAE devrait pouvoir cumuler les statistiques de révision pour une période donnée et établir un tableau et un graphique sur cette activité.	0
<b>9.2.29</b>	Le SAE devrait pouvoir cumuler les statistiques de décision et de levée de gel de destruction pour une période donnée et établir un tableau et un graphique sur cette activité.	P
<b>9.2.30</b>	Le SAE doit produire un rapport détaillant les anomalies en cas de transfert, d'export, de destruction ou de suppression. Le rapport doit identifier les documents, groupes et métadonnées associées à transférer dont le traitement a provoqué une erreur, et toute entité dont le transfert, l'export, la destruction ou la suppression a échoué.	0
<b>9.2.31</b>	Le SAE doit produire un rapport détaillant les anomalies en cas d'import. Le rapport doit identifier les documents, groupes et métadonnées associées à importer dont le traitement a provoqué une erreur, et toute entité dont l'import a échoué.	0
<b>9.2.32</b>	Le SAE devrait assister le processus d'import, en traçant la progression et l'état de l'import, y compris le pourcentage d'exécution et le nombre de documents importés.	0
<b>9.2.33</b>	Le SAE devrait permettre de trier une sélection de dossiers à transférer dans l'ordre des différentes métadonnées définies par les utilisateurs.	0
<b>9.2.34</b>	Le SAE devrait permettre de créer des formulaires définis par les utilisateurs pour décrire les dossiers et documents électroniques à exporter ou à transférer.	0

## 9.3 MODIFICATION, SUPPRESSION ET MASQUAGE DES DOCUMENTS ARCHIVES

---

Un des fondamentaux de l'archivage est que, normalement, les documents archivés ne peuvent pas être modifiés, et (sauf à la fin de leur cycle de vie dans le SAE) les dossiers, sous-dossiers, volumes et documents ne peuvent pas être détruits.

Cette section traite des exigences relatives aux cas exceptionnels où le contenu d'un document archivé doit être corrigé, ou quand un document doit être supprimé et remplacé.

Dans certains cas, les administrateurs peuvent avoir besoin de « supprimer » des documents pour corriger des erreurs afin de se conformer aux exigences légales, par suite de la législation sur la protection des données personnelles ou pour d'autres raisons.

L'action de suppression peut signifier deux choses :

- destruction ;
- conservation avec mention dans les métadonnées que le document est virtuellement absent et doit être ignoré.

Autrement, la suppression doit être exceptionnelle et cette possibilité doit être strictement contrôlée afin de protéger l'intégrité générale des documents. Les suppressions doivent notamment être tracées dans l'historique des événements.

*Si les exigences de la réglementation ou de la législation locales sont différentes, par exemple sur la purge des données personnelles (voir ISO 12037), cela sera précisé dans le chapitre zéro.*

Les administrateurs ont parfois besoin de publier, ou de rendre accessibles, des documents comportant des informations encore sensibles, sans révéler ces informations sensibles, par suite de la protection des données, de considérations liées à la sécurité, du risque commercial, etc. C'est pourquoi les administrateurs peuvent avoir besoin de masquer l'information sensible, sans altérer le document initial.

Ce procédé est appelé ici « masquage ». Quand on applique ce procédé, il en résulte d'une part le document original (inchangé), d'autre part une copie du document partiellement masqué (la copie [masquée](#) ou extrait du document original). Le SAE conserve les deux (document original et extrait).

En principe, le masquage peut s'appliquer à toute nature de document archivé - texte, image, audio, vidéo, etc.

A noter que la suppression et la modification sont également abordées au chapitre 5.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>9.3.1</b>	<p>Le SAE doit proposer une option de configuration qui interdit qu'un document, une fois capturé, soit supprimé ou déplacé par un administrateur ou un utilisateur ; voir aussi 9.3.3.</p> <p><i>Cette exigence ne doit pas affecter le transfert ou la destruction des documents en application des règles de conservation/destruction (voir section 5.3). Elle vise les cas où la suppression des documents archivés (voir ci-dessus) est inutile ou interdite. Une alternative est proposée en 9.3.2.</i></p>	O

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>9.3.2</b>	<p>Le SAE devrait proposer une option de configuration, alternative à 9.3.1, où la suppression d'un document correspond à sa destruction, et où son reclassement équivaut à un déplacement ; voir aussi 9.3.1.</p> <p><i>Ce ne sont pas là de bonnes pratiques de l'archivage. Ce point ne concerne que les situations où on ne peut faire autrement. En général, l'option indiquée en 9.3.1 est préférable. Les options 9.3.1 et celle-ci sont exclusives.</i></p>	0
<b>9.3.3</b>	<p>Si l'option 9.3.1 est retenue, le SAE doit se comporter comme suit :</p> <ul style="list-style-type: none"><li>• si un administrateur « supprime » un document (comme dans 9.3.5), ses métadonnées doivent être mises à jour en conséquence ; le SAE doit cacher le contenu et les métadonnées à tous les utilisateurs (sauf éventuellement des administrateurs dûment autorisés), comme s'il était supprimé, et tracer l'opération dans l'historique.</li><li>• si un administrateur « reclasse » un document (comme en 9.3.5), le SAE doit réagir comme lors d'une suppression avec, en plus, l'insertion automatique d'une copie (ou d'un pointeur, selon la méthode de stockage utilisée) au nouvel emplacement.</li></ul> <p><i>Cela suppose que très peu d'administrateurs voire aucun n'aurait cette autorisation.</i></p>	0
<b>9.3.4</b>	<p>Si l'option 9.3.2 est retenue, le SAE doit se comporter comme suit :</p> <ul style="list-style-type: none"><li>• si un administrateur supprime un document (voir 9.3.2), le document doit être détruit avec ses métadonnées, sauf les métadonnées retenues comme métadonnées-témoins (voir 9.3.5) ; le SAE doit enregistrer l'opération dans l'historique.</li><li>• si un administrateur reclasse un document (voir 9.3.5), le SAE doit réagir comme lors d'une suppression mais en intégrant automatiquement le document (ou son pointeur, selon la méthode de stockage utilisée) au nouvel emplacement.</li></ul>	0
<b>9.3.5</b>	<p>Le SAE doit permettre aux administrateurs de supprimer des séries, dossiers, sous-dossiers, volumes et documents en dehors du processus de révision.</p> <p><i>Ce point ne concerne que les cas exceptionnels cités dans cette section. A rapprocher de 9.3.1 et 9.3.2.</i></p>	0
<b>9.3.6</b>	<p>Le SAE doit permettre aux utilisateurs de proposer des séries, dossiers, sous-dossiers, volumes et documents à la suppression.</p> <p><i>L'administrateur peut alors décider d'effectuer ou non la suppression.</i></p>	0

Réf	Exigence	Test
9.3.7	<p>En cas de suppression de ce type, le SAE doit :</p> <ul style="list-style-type: none"> <li>• enregistrer la suppression dans l'historique des événements ;</li> <li>• envoyer un rapport aux administrateurs ;</li> <li>• supprimer la totalité du contenu d'une série, d'un dossier, sous-dossier ou volume supprimé ;</li> <li>• s'assurer qu'aucun document dont la suppression affecterait un autre document archivé n'est supprimé (cas d'une pièce appartenant à deux documents dont l'un serait supprimé) ;</li> <li>• signaler aux administrateurs tout lien avec un autre dossier, ou entre un document et un dossier, sous-dossier ou volume en passe d'être supprimé, et demander une confirmation avant de poursuivre la suppression ;</li> <li>• maintenir en tout temps l'intégrité des métadonnées.</li> </ul> <p><i>Ici l'expression « maintenir l'intégrité des métadonnées » signifie s'assurer qu'aucune métadonnée d'une entité (série, document, etc.) ne renvoie à une entité inexistante.</i></p>	O
9.3.8	<p>Les administrateurs doivent pouvoir modifier une métadonnée saisie par un utilisateur.</p> <p><i>Cette fonctionnalité doit permettre aux administrateurs de corriger les erreurs des utilisateurs (erreur de saisie, etc.) et de maintenir les accès des utilisateurs et des groupes. Les bonnes pratiques veulent que les utilisateurs corrigent eux-mêmes leurs erreurs ; cette exigence ne les en dispense pas.</i></p>	O
9.3.9	<p>Toutes les modifications apportées aux métadonnées doivent être tracées dans l'historique.</p>	O
9.3.10	<p>Le SAE doit permettre aux administrateurs de créer un ou plusieurs extraits d'un document qu'il convient de masquer, tout en conservant l'original.</p> <p><i>Il peut s'avérer nécessaire de fournir plusieurs extraits d'un document dont des passages différents ont dû être masqués.</i></p>	O
9.3.11	<p>Le SAE doit permettre de retirer ou de cacher les informations sensibles dans un extrait pour tous les formats d'archivage préconisés.</p> <p><i>Si le SAE n'offre pas cette fonction, il doit favoriser l'intégration d'un autre logiciel capable de le faire. On peut admettre que le SAE convertisse un document dans un format de fichier différent pour permettre le masquage d'une copie, si la conversion garantit une fidélité suffisante.</i></p> <p><i>Il est essentiel, en cas de recours à l'une ou l'autre fonction de masquage, que les informations retirées ou cachées ne puissent en aucun cas être récupérées à partir de l'extrait, ni à l'écran ni à l'impression ni par rejeu, ni sous aucune forme, sans parler de l'utilisation des fonctions de rotation, de zoom ou de quelque manipulation que ce soit, y compris la restitution de l'extrait avec un autre logiciel.</i></p>	P

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>9.3.12</b>	Quand un extrait est créé, le SAE doit automatiquement enregistrer sa création dans les métadonnées de l'extrait et du document (date, heure, auteur, etc.).	O
<b>9.3.13</b>	Quand un extrait est créé, le SAE doit demander à l'utilisateur concerné d'en saisir le motif et doit conserver cette donnée dans les métadonnées de l'extrait et du document.	O
<b>9.3.14</b>	En cas de création d'extrait, le SAE devrait déclarer et archiver automatiquement les extraits en tant que tels et les classer dans le même groupe que l'original, en demandant à l'auteur : <ul style="list-style-type: none"> <li>• un motif (voir 9.3.13) ;</li> <li>• un niveau de sécurité (le cas échéant) ;</li> <li>• éventuellement, un groupe de documents où la copie de l'extrait sera déclarée.</li> </ul>	P
<b>9.3.15</b>	En cas de création d'extrait, le SAE devrait permettre de recopier les métadonnées pour l'extrait.	O
<b>9.3.16</b>	Sous réserve des droits d'accès, le SAE devrait permettre de corriger certaines métadonnées, notamment le titre.	O
<b>9.3.17</b>	Le SAE devrait conserver une référence à un extrait dans la même série, le même dossier, sous-dossier ou volume que le document d'origine, même si cette entité est close.  <i>Ceci complète l'exigence de classement d'une copie (voir 9.3.13), en permettant les références croisées au sein d'un même dossier, au cas où original et extrait sont séparés par un grand nombre de documents dans le dossier.</i>	O
<b>9.3.18</b>	Quand un document est repéré, le SAE doit indiquer, ou permettre à l'utilisateur de voir, l'existence de tous les extraits qui en ont été faits et, selon les contrôles d'accès et de sécurité, les rendre accessibles.	O
<b>9.3.19</b>	Quand un extrait est repéré, le SAE doit indiquer, ou permettre à l'utilisateur de voir, l'existence du document d'origine et, selon les contrôles d'accès et de sécurité, les rendre accessibles.	O
<b>9.3.20</b>	Le SAE doit conserver dans l'historique toute modification effectuée en application d'une exigence de cette section.	P

## 10. Modules optionnels

Ce chapitre présente des exigences fonctionnellement très proches de l'archivage électronique, à savoir les fonctionnalités de gestion des documents archivés sous forme papier (non électronique), de GED, de workflow, de signature électronique et autres.

Chaque section du chapitre correspond à un module optionnel du cadre de tests de MoReq2. Ces modules sont optionnels dans le sens où leurs exigences ne font pas partie du noyau de fonctionnalités obligatoires d'un SAE conforme à MoReq2.

Les exigences de ce chapitre couvrent les domaines suivants :

- gestion des archives physiques (section 10.1) ;
- destruction des archives physiques (section 10.2) ;
- GED et travail collaboratif (section 10.3) ;
- workflow (section 10.4) ;
- gestion de dossiers sériels (section 10.5) ;
- intégration avec les systèmes de gestion de contenu (section 10.6) ;
- signature électronique (section 10.7) ;
- chiffrement (section 10.8) ;
- gestion des droits numériques (section 10.9) ;
- systèmes distribués (section 10.10) ;
- travail hors ligne et à distance (section 10.11) ;
- intégration du fax (section 10.12) ;
- niveaux de sécurité (section 10.13) ;

Les exigences de ce chapitre visent des fonctions optionnelles qui peuvent être intégrées à un SAE. Elles viennent compléter le noyau dur des exigences de MoReq2. Elles ne sont applicables que si l'entreprise/organisation en a besoin.

La conformité à MoReq2 n'implique pas de satisfaire à ces exigences. Toutefois, si le module optionnel auquel elles sont rattachées fait partie d'un test, elles sont obligatoires.

Dans tous les cas, le niveau avancé pour ces exigences est élevé. Dans la mesure où elles ne définissent pas les fonctions principales d'un SAE, elles ne sont pas exhaustives mais documentent les opérations appropriées.

## 10.1 GESTION DES ARCHIVES PHYSIQUES (NON ELECTRONIQUES)

---

A côté des archives électroniques, les locaux d'archivage d'une entreprise/organisation peuvent conserver des archives non électroniques. Ce peut être des archives papier ou sur d'autres supports analogiques, par exemple des microfiches ou des bandes audio. Ce peut être également des archives numériques stockées sur des supports amovibles tels que cédéroms, DVD ou bandes.

L'adjectif « physique » est utilisé par MoReq2 pour désigner tout document archivé sur un support extérieur au SAE, c'est-à-dire non seulement les supports analogiques mais aussi les supports numériques contenant des documents qui ne sont pas contrôlés individuellement par le SAE. Exemple :

- un cédérom contenant 10 000 images qui ne sont pas individuellement reconnues et gérées par le SAE est une entité physique ;
- un cédérom contenant 10 000 images stocké dans un lecteur ou un jukebox connecté au SAE et dont chaque image a été archivée et est gérée par le SAE n'est pas une entité physique - c'est un support amovible où sont stockés des documents électroniques.

Ces spécifications ne traitent pas des besoins métier de gérer et de conserver des archives physiques. Ce besoin peut exister ou non, selon l'environnement législatif et réglementaire. S'il existe, il faut veiller à préserver l'intégrité et l'accessibilité des archives électroniques et physiques comme un tout. Ces questions seront gérées par des procédures organisationnelles spécifiques.

Le SAE doit pouvoir gérer les références aux archives physiques et/ou électroniques ; il doit pouvoir gérer des unités mixtes constituées d'archives électroniques et d'archives physiques. Les séries, dossiers, sous-dossiers et volumes peuvent comporter toute combinaison de documents physiques et électroniques. Ce point diffère du modèle relationnel des entités de la version précédente de MoReq.

Les documents physiques peuvent coexister avec les documents électroniques de plusieurs manières, notamment :

- une série, un dossier, sous-dossier ou volume ne contient que des documents physiques ; dans ce cas, l'entité identifiée dans le SAE renvoie à un contenant physique, par exemple une chemise de classement ;
- une série, un dossier, sous-dossier ou volume mêle documents physiques et électroniques ; le contenant physique des documents n'est pas significatif pour l'archivage - par exemple un dessin d'ingénierie stocké dans un classeur avec d'autres dessins sur d'autres sujets.

Le SAE doit fournir des fonctions de gestion des contenants physiques (premier cas).

Pour gérer les documents physiques, le SAE doit pouvoir capturer et gérer leurs métadonnées. Ces métadonnées permettent aux administrateurs et aux utilisateurs, sous réserve des droits d'accès, de localiser, suivre, retrouver, réviser et détruire les documents physiques, et de leur attribuer des droits d'accès de la même façon que pour les documents électroniques.

De la même façon, le SAE doit pouvoir capturer et gérer les métadonnées des contenants physiques.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
10.1.1	Le SAE doit permettre à un administrateur d'identifier les séries, dossiers, sous-dossiers et volumes correspondant à des contenants physiques.	0

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
10.1.2	Le SAE doit permettre aux administrateurs et aux utilisateurs de saisir et de gérer les métadonnées relatives aux séries, dossiers, sous-dossiers et volumes qui existent sous forme de contenants physiques, conformément au modèle de métadonnées de MoReq2.	O
10.1.3	Le SAE doit permettre aux utilisateurs de saisir et de gérer la description des documents physiques dans des séries, dossiers, sous-dossiers et volumes, avec les mêmes règles que pour la capture des documents électroniques.	O
10.1.4	Le SAE doit permettre de mêler et de combiner les documents physiques et électroniques dans une série, un dossier, sous-dossier ou volume.	O
10.1.5	Le SAE doit permettre de gérer les documents physiques de la même façon que les documents électroniques, y compris l'héritage des métadonnées.	P
10.1.6	Lorsqu'un utilisateur recherche, repère ou travaille sur une série, un dossier, sous-dossier ou volume, le SAE devrait lui signaler la présence de tout contenant ou document physique avec les indicateurs appropriés.  <i>Il faut qu'un utilisateur puisse savoir facilement s'il existe des entités physiques afin de s'assurer que tous les documents sont gérés de la même manière. MoReq2 ne définit pas la nature de ces indicateurs.</i>	O
10.1.7	Le SAE doit permettre à un administrateur d'attribuer aux séries, dossiers, sous-dossiers ou volumes physiques un jeu de métadonnées différent des documents électroniques. Par exemple, les métadonnées d'un dossier physique pourront être complétées par les métadonnées suivantes (entre autres) : <ul style="list-style-type: none"> <li>• information sur la localisation physique ;</li> <li>• information sur le format du contenant ou du document physique.</li> </ul>	O
10.1.8	Le SAE doit s'assurer que le repérage d'une série, d'un dossier, sous-dossier ou volume s'applique, en même temps et en une seule opération, aux métadonnées des entités tant physiques qu'électroniques qui en relèvent.	O
10.1.9	Le SAE devrait faciliter la traçabilité des contenants et documents physiques par la saisie des dates d'emprunt et de retour, de la localisation des documents, du <a href="#">responsable du stockage</a> .	O
10.1.10	Le SAE devrait permettre à l'utilisateur qui emprunte un ou plusieurs documents physiques d'indiquer une date prévue de retour.	O
10.1.11	Quand la date de retour prévue d'un ou plusieurs documents physiques approche ou est dépassée, le SAE devrait alerter l'utilisateur concerné.	O
10.1.12	Le SAE devrait permettre à un utilisateur dûment autorisé de modifier la date prévue du retour d'un ou plusieurs documents physiques, en une seule opération.	O
10.1.13	Le SAE doit garantir que les métadonnées des documents physiques sont systématiquement soumises aux mêmes contrôles d'accès que si ces documents étaient entièrement électroniques.	O

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
10.1.14	Le SAE devrait fournir une fonction de suivi pour permettre à l'utilisateur de tracer la localisation et les mouvements des documents physiques.	0
10.1.15	La fonction de suivi des mouvements du SAE devrait permettre de sélectionner la localisation des documents physiques, ou de la valider, dans une liste (menu déroulant).  <i>Si le SAE ne contient pas la liste des localisations, on peut accepter une saisie en texte libre.</i>	0
10.1.16	La fonction de suivi des mouvements du SAE doit permettre à l'utilisateur d'enregistrer l'emprunt et le retour des documents physiques.  <i>Autrement dit, le SAE doit fournir le moyen de tracer si le document physique est à sa place ou s'il est sorti.</i>	0
10.1.17	La fonction de suivi du SAE doit enregistrer les données relatives aux mouvements d'une entité physique, à savoir : <ul style="list-style-type: none"> <li>• identifiant unique ;</li> <li>• localisation de référence ;</li> <li>• nombre de localisations précédentes (défini par un administrateur au moment de la configuration) ;</li> <li>• date de sortie (emprunt) ;</li> <li>• date de retour ;</li> <li>• gestionnaire du mouvement (le cas échéant).</li> </ul>	0
10.1.18	Le SAE doit permettre à un utilisateur de voir la localisation d'une entité empruntée, le responsable du stockage et la date de l'emprunt, sous réserve des droits d'accès.	0
10.1.19	Le SAE doit tracer tous les emprunts et tous les retours dans l'historique des événements.	0
10.1.20	Le SAE doit pouvoir enregistrer dans l'historique toutes les modifications apportées aux métadonnées des documents physiques.  <i>Exemple : métadonnée de localisation.</i>	0
10.1.21	Le SAE devrait faciliter l'impression et la reconnaissance de codes-barres pour les dossiers, sous-dossiers, volumes et documents, ou un autre système de traçabilité, tel que la technologie RFID (Radio Frequency Identification).  <i>C'est un moyen de tracer la localisation et les mouvements des documents physiques.</i>	0
10.1.22	Le SAE devrait faciliter l'impression d'étiquettes pour les dossiers, sous-dossiers et volumes.	0

Réf	Exigence	Test
	<p>Il s'agit de produire une étiquette comportant les métadonnées essentielles d'une entité physique, à savoir (liste non exhaustive) :</p> <ul style="list-style-type: none"> <li>• titre ;</li> <li>• identifiant système ;</li> <li>• code de classement ;</li> <li>• date d'ouverture ;</li> <li>• niveau de sécurité (le cas échéant) ;</li> <li>• localisation courante.</li> </ul>	
10.1.23	<p>Le SAE doit se comporter de la même façon dans la recherche de documents papier et de documents électroniques, à ceci près que :</p> <ul style="list-style-type: none"> <li>• le contenu des documents physiques ne peut être restitué à l'écran (à la place, le SAE affiche les métadonnées de localisation, voir ci-dessous) ;</li> <li>• les métadonnées affichées peuvent différer entre documents physiques et électroniques.</li> </ul>	0
10.1.24	<p>Le SAE devrait pouvoir signaler aux administrateurs toute application des règles de conservation/destruction aux documents ou groupes de documents physiques intervenue depuis la restauration.</p> <p><i>La section 4.3 « Sauvegarde et restauration » présente les exigences de restauration d'un SAE. Si le système gère également les documents non électroniques, des disparités peuvent apparaître après une restauration si des destructions ont eu lieu pour les documents physiques et que le SAE ne l'indique pas. Cette exigence permet aux administrateurs d'effectuer une action corrective.</i></p>	0

## 10.2 DESTRUCTION DES ARCHIVES PHYSIQUES

Réf	Exigence	Test
10.2.1	<p>Quand une durée de conservation arrive à échéance, en application d'une règle de conservation/destruction, et qu'elle vise des entités physiques, le SAE doit alerter un administrateur.</p>	0
10.2.2	<p>Le SAE doit avertir un administrateur de l'existence et de la localisation de toute entité physique relevant d'une série, d'un dossier, sous-dossier ou volume devant être transféré, exporté ou détruit.</p> <p><i>Ceci peut survenir à échéance d'une règle de conservation/destruction ou quand un transfert ou un export est décidé.</i></p>	0

Réf	Exigence	Test
10.2.3	Lors de l'export ou du transfert d'entités physiques, le SAE doit exporter ou transférer leurs métadonnées de la même manière que les métadonnées des documents électroniques.	0
10.2.4	En cas d'export, transfert ou destruction d'entités physiques, le SAE doit demander à un administrateur de confirmer le transfert, l'export ou la destruction physique avant de parachever ces opérations.  <i>L'administrateur devra en général saisir manuellement la confirmation que les documents physiques ont bien été transférés ou détruits.</i>	0

## 10.3 GESTION ELECTRONIQUE DE DOCUMENTS ET TRAVAIL COLLABORATIF

---

Les systèmes de gestion électronique de documents - GED - sont largement utilisés dans les entreprises/organisations pour assurer la gestion et le contrôle des documents électroniques. De nombreuses fonctionnalités d'outils de GED recouvrent celles d'un SAE. Un outil de GED offre notamment l'indexation des documents, la gestion du stockage, le contrôle des versions, une intégration avec les applications bureautiques et des outils de recherche pour accéder aux contenus. Certains SAE proposent des fonctions de GED complètes, d'autres une partie seulement. Inversement, certains outils de GED ont intégré les principales fonctions d'archivage.

Les systèmes de GED sont souvent intégrés dans un système d'information plus vaste et incluent des outils collaboratifs qui permettent à un ensemble d'utilisateurs de participer à l'élaboration d'un document.

Le travail collaboratif est aussi une composante des systèmes de gestion de contenu. Voir la section 10.6 pour plus de détails sur ces aspects.

Pour clarifier les choses, le tableau ci-après montre les différences caractéristiques entre un système de GED et un SAE.

Un système de GED...	Un SAE...
<ul style="list-style-type: none"> <li>• permet la modification des documents ;</li> </ul>	<ul style="list-style-type: none"> <li>• interdit la modification des documents archivés ;</li> </ul>
<ul style="list-style-type: none"> <li>• permet la coexistence de plusieurs versions d'un même document ;</li> </ul>	<ul style="list-style-type: none"> <li>• admet que seule la version finale d'un document soit archivée</li> </ul>
<ul style="list-style-type: none"> <li>• peut permettre la destruction des documents par leurs propriétaires ;</li> </ul>	<ul style="list-style-type: none"> <li>• interdit la destruction des documents archivés en dehors de certains cas strictement contrôlés ;</li> </ul>
<ul style="list-style-type: none"> <li>• peut comporter des règles de conservation ;</li> </ul>	<ul style="list-style-type: none"> <li>• comprend obligatoirement un contrôle rigoureux des durées de conservation ;</li> </ul>

Un système de GED...	Un SAE...
<ul style="list-style-type: none"> <li>peut comprendre une structure organisée de stockage, sous le contrôle des utilisateurs ;</li> </ul>	<ul style="list-style-type: none"> <li>comprend obligatoirement une structure rigoureuse de classement (le plan de classement), gérée et contrôlée par l'administrateur ;</li> </ul>
<ul style="list-style-type: none"> <li>est a priori dédié à la gestion quotidienne des documents pour la conduite des affaires.</li> </ul>	<ul style="list-style-type: none"> <li>peut supporter les tâches quotidiennes mais est d'abord destiné à la constitution d'un fonds sécurisé des documents probants.</li> </ul>

La suite de cette section présente les exigences clés pour promouvoir une solution intégrée SAE/GED. Les exigences ne visent que les outils de GED intégrés à un SAE. Une des caractéristiques est l'idée que les documents de travail peuvent être stockés (classés) dans les mêmes séries et dossiers que les documents à archiver, bien que ceci soit facultatif. Cela permet de classer les projets dans le même dossier que les versions finales qui seront, elles, archivées.

A noter que le mot « document de travail » est utilisé ici pour décrire une information ou un objet qui n'a pas été déclaré ni archivé dans le SAE.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>10.3.1</b>	<p>Le SAE devrait pouvoir gérer les documents de travail électroniques et les documents archivés avec le même plan de classement et les mêmes mécanismes de contrôle d'accès.</p> <p><i>Le but de cette exigence est de permettre aux utilisateurs de stocker les documents en cours d'élaboration dans les mêmes dossiers que les documents archivés. Ceci est optionnel.</i></p>	0
<b>10.3.2</b>	<p>Si le SAE gère des documents de travail et des documents archivés avec le même plan de classement, il doit clairement indiquer quels sont les documents de travail et quels sont les documents archivés.</p> <p><i>MoReq2 ne précise pas comment procéder.</i></p>	0
<b>10.3.3</b>	<p>Si le SAE gère des documents de travail et des documents archivés avec le même plan de classement, il doit permettre aux utilisateurs d'effectuer une des actions suivantes sur une série ou un dossier :</p> <ul style="list-style-type: none"> <li>archiver tous les documents de travail ;</li> <li>détruire tous les documents de travail en ne laissant que les documents archivés ;</li> <li>détruire tous les documents de travail qui ont plus de tel âge.</li> </ul>	0

Réf	Exigence	Test
10.3.4	<p>Si le SAE gère des documents de travail et des documents archivés avec le même plan de classement, il doit signaler à un administrateur l'existence de documents de travail dans une série ou un dossier à exporter et permettre une des options suivantes :</p> <ul style="list-style-type: none"> <li>détruire des documents de travail ;</li> <li>archiver les documents de travail ;</li> <li>les exporter avec les documents archivés.</li> </ul>	O
10.3.5	<p>Quand une GED est intégrée dans le SAE, ou partiellement intégrée, elle doit être capable de pousser automatiquement les documents électroniques élaborés par les équipes métiers vers le SAE pour capture et archivage automatique.</p> <p><i>Ceci concerne plus particulièrement la gestion de dossiers sériels, voir aussi section 10.5</i></p>	P
10.3.6	<p>Le SAE doit permettre aux utilisateurs :</p> <ul style="list-style-type: none"> <li>de capturer un document électronique et de l'archiver en une seule opération ;</li> </ul> <p>ou</p> <ul style="list-style-type: none"> <li>de capturer un document électronique, de le stocker, et de poursuivre plus tard le processus d'archivage.</li> </ul>	O
10.3.7	<p>Le SAE doit pouvoir copier le contenu d'un document électronique archivé afin de créer un nouveau document sans forcément archiver cette copie, et sans affecter la conservation de l'original.</p> <p><i>Exemple : un utilisateur fait une copie d'un document archivé à destination de quelqu'un qui n'a pas accès au SAE. Selon le contexte, cette copie sera ou ne sera pas archivée en tant que telle.</i></p>	O
10.3.8	<p>Le SAE doit permettre aux utilisateurs d'emprunter tout document de travail auquel ils ont le droit d'accéder.</p>	O
10.3.9	<p>Le SAE doit permettre aux utilisateurs de restituer un document emprunté soit dans le même état soit en le déclarant comme nouvelle version (voir 10.3.20).</p>	O
10.3.10	<p>Le SAE devrait permettre à un utilisateur qui restitue un document de saisir, s'il le souhaite, un commentaire sur les modifications apportées pendant l'emprunt.</p>	O
10.3.11	<p>Quand un document est emprunté par un utilisateur, le SAE doit interdire qu'un autre utilisateur puisse l'emprunter ou le modifier (voir aussi 10.3.13).</p> <p><i>Pendant un emprunt, seul l'utilisateur qui a effectué l'emprunt peut modifier le document.</i></p> <p><i>Seuls les documents de travail sont concernés. Par définition, le SAE ne doit autoriser aucun emprunt ni aucune correction sur un document archivé.</i></p>	O

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>10.3.12</b>	<p>Pendant un emprunt, si un autre utilisateur tente d'emprunter le même document, le SAE doit l'en empêcher en l'informant que celui-ci est déjà sorti. Ce faisant, le SAE peut :</p> <ul style="list-style-type: none"> <li>• indiquer l'identité de l'emprunteur ;</li> </ul> <p>ou</p> <ul style="list-style-type: none"> <li>• masquer l'identité de l'emprunteur ;</li> </ul> <p>option à définir au moment de la configuration.</p>	O
<b>10.3.13</b>	<p>Le SAE doit permettre à un administrateur d'annuler l'emprunt d'un document de travail.</p> <p>Il s'agit des cas où l'utilisateur emprunteur est dans l'impossibilité de le restituer. Ceci peut se produire pour diverses raisons, par exemple :</p> <ul style="list-style-type: none"> <li>• l'utilisateur a transféré le document vers un poste de travail tombé en panne ou volé ;</li> <li>• le document emprunté a été corrompu ;</li> <li>• l'utilisateur a oublié de le restituer avant de partir en congés.</li> </ul>	O
<b>10.3.14</b>	<p>Un utilisateur ne doit pas pouvoir restituer une version de document dont l'emprunt a été annulé (10.3.13) comme étant le même document.</p>	O
<b>10.3.15</b>	<p>Si quelqu'un tente d'archiver dans le SAE un groupe de documents comportant un document emprunté, l'anomalie doit être signalée à un administrateur.</p>	O
<b>10.3.16</b>	<p>Les utilisateurs devraient pouvoir capturer un document à partir de l'outil de GED.</p>	O
<b>10.3.17</b>	<p>Les utilisateurs doivent pouvoir glisser facilement les documents entre l'outil de GED et le SAE pour les déclarer à l'archivage.</p> <p><i>Ce point est particulièrement important lorsque l'outil GED/SAE est utilisé dans un environnement bureautique.</i></p>	N
<b>10.3.18</b>	<p>Lorsqu'un document existe en plusieurs versions, le SAE doit être en mesure d'effectuer la capture et l'archivage de toutes les manières suivantes, l'une étant retenue par défaut au moment de la configuration, avec la possibilité pour l'utilisateur de choisir :</p> <ul style="list-style-type: none"> <li>• la version la plus récente ;</li> <li>• la version sélectionnée par l'utilisateur ;</li> <li>• toutes les versions, archivées comme un seul document ;</li> <li>• toutes les versions, archivées comme autant de documents individuels mais reliés.</li> </ul>	O
<b>10.3.19</b>	<p>Le SAE doit conserver un numéro de version pour chaque document, et doit le faire apparaître clairement en cas de recherche ou de repérage du document.</p>	O
<b>10.3.20</b>	<p>Le SAE doit automatiquement incrémenter le numéro de version quand un document est restitué comme nouvelle version.</p>	O

Réf	Exigence	Test
10.3.21	<p>Le SAE devrait permettre de définir le système de numérotation des versions au moment de la configuration, avec au minimum une de ces deux options :</p> <ul style="list-style-type: none"> <li>• simple numérotation séquentielle (1, 2, 3, etc.) ;</li> <li>• numérotation des versions majeures et mineures, c'est-à-dire numéros de type x.y où x indique une version majeure et y une version mineure, selon le choix de l'utilisateur, la version mineure revenant automatiquement à 0 quand la version majeure est incrémentée.</li> </ul> <p><i>D'autres systèmes de numérotation sont possibles.</i></p>	O
10.3.22	<p>Le SAE doit permettre à un administrateur de configurer le stockage des versions, au moment de la configuration ou plus tard, au niveau de la série ou du dossier, avec au moins les options suivantes pour chaque série ou dossier :</p> <ul style="list-style-type: none"> <li>• toutes les versions de tous les documents sont stockées dans la série ou le dossier ;</li> <li>• seule la version la plus récente d'un document (si un administrateur a la possibilité d'indiquer les versions majeures et mineures) est stockée dans la série ou le dossier ;</li> <li>• le nombre de versions qu'on peut stocker dans une série ou un dossier est défini par un administrateur.</li> </ul> <p><i>Ceci doit permettre le contrôle des versions si l'historique de l'élaboration du document est demandé. Quand cet historique n'est pas nécessaire, le nombre des versions stockées - et la capacité de stockage - peuvent être réduits.</i></p>	O
10.3.23	<p>Le SAE devrait permettre à l'utilisateur qui stocke un document de ne pas tenir compte des valeurs par défaut pour le nombre de versions à stocker (voir 10.3.22).</p>	O
10.3.24	<p>Le SAE doit permettre à un utilisateur de saisir les métadonnées du document archivé au moment de la capture.</p>	O
10.3.25	<p>Le SAE doit garantir que toute métadonnée capturée est gérée conformément au modèle de métadonnées de MoReq2.</p>	O
10.3.26	<p>Le SAE devrait permettre à un utilisateur autorisé de comparer les métadonnées de la GED avec les champs appropriés du SAE.</p>	N
10.3.27	<p>En cas de contradiction entre les métadonnées du SAE et celles du système de production, le SAE doit alerter l'utilisateur.</p> <p><i>Ceci peut arriver quand le SAE ne contrôle pas les métadonnées du document.</i></p>	O
10.3.28	<p>Le SAE devrait être en mesure d'intégrer les nouvelles versions ou systèmes de GED dès leur mise en service dans l'entreprise/organisation.</p> <p><i>MoReq2 n'indique pas comment procéder. Les entreprises/organisations devront étudier cette question plus à fond.</i></p>	N
10.3.29	<p>Le SAE doit pouvoir gérer le contrôle des versions, c'est-à-dire gérer différentes versions d'un même document électronique comme une seule entité.</p>	O

Réf	Exigence	Test
	<i>Ceci pour faciliter le processus de rédaction et permettre le travail collaboratif.</i>	
10.3.30	Le SAE devrait pouvoir limiter la consultation des utilisateurs à : <ul style="list-style-type: none"><li>• uniquement la dernière version d'un document ;</li><li>• une sélection de versions ;</li><li>• toutes les versions du document ;</li><li>• les versions capturées et archivées ;</li><li>• selon le choix opéré par un administrateur au moment de la configuration ou plus tard.</li></ul>	0
10.3.31	Le SAE devrait permettre aux utilisateurs d'avoir un espace personnel pour leurs documents de travail.  Il s'agit de permettre aux utilisateurs de stocker des documents « personnels » qui ne sont pas destinés à être archivés, par exemple, des brouillons qu'il n'y a aucun intérêt à partager ou d'autres documents. Cet espace de travail devrait être optionnel (c'est-à-dire qu'au moment de la configuration du SAE, on peut le supprimer).	0
10.3.32	Si le SAE comprend un espace de travail personnel, un administrateur doit fixer une taille limite par utilisateur.	0
10.3.33	Si le SAE comprend un espace de travail personnel, son accès doit être réservé à son propriétaire.	0

## 10.4 WORKFLOW

---

La Workflow Management Coalition (WfMC) - une association internationale pour le développement des normes de workflow - définit le workflow comme « l'automatisation de tout ou d'une partie d'un processus métier, au cours duquel les documents, l'information ou les tâches passent d'un participant à l'autre, pour action, en application de procédures préétablies ». Dans cette définition, un « participant » peut être un utilisateur ou un groupe (une équipe), ou une application informatique.

Les exigences de cette section couvrent les fonctions de base (décrites en 6.1.35) ainsi que des fonctionnalités plus élaborées de workflow telles que la gestion d'un fort volume de transactions avec des cas particuliers, reporting, performance individuelle. Ces dernières peuvent être fournies par l'intégration d'une solution de workflow au SAE.

La technologie de workflow fait passer les objets électroniques entre les participants grâce à un programme de contrôle automatique. Dans le contexte d'un SAE, le workflow est utilisé pour faire circuler les dossiers et documents, archivés ou non, entre utilisateurs, services et applications. Il sert normalement à :

- gérer les tâches délicates telles que l'enregistrement et le processus de destruction des dossiers ou documents ;

- vérifier et approuver les documents avant leur archivage ;
- contrôler le routage des documents ou dossiers d'un utilisateur à l'autre pour action (vérification du document, approbation de nouvelle version) ;
- signaler aux utilisateurs la disponibilité des documents ;
- diffuser les documents ;
- organiser le processus de gestion de dossiers sériels.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
10.4.1	Le SAE doit permettre les workflows, c'est-à-dire des enchaînements de tâches, chaque tâche consistant (par exemple) à passer une pièce, un document ou un dossier d'un participant à l'autre pour action ou décision.	O
10.4.2	Le SAE doit reconnaître comme participants aussi bien les utilisateurs que les groupes de travail.	O
10.4.3	Quand le participant est un groupe, le workflow du SAE devrait inclure le moyen de distribuer les éléments entrants entre les membres du groupe à tour de rôle et, si un membre est occupé, de le basculer sur un autre.	O
10.4.4	Le SAE doit permettre aux administrateurs de prédéfinir des workflows.	O
10.4.5	Le SAE doit permettre aux administrateurs de sauvegarder des workflows pour une utilisation future.	O
	<i>Ceci suppose d'attribuer un identifiant à chaque workflow sauvegardé.</i>	
10.4.6	Le SAE devrait permettre à l'administrateur qui sauvegarde un workflow de lui attribuer un intitulé en texte libre.	O
10.4.7	Le SAE doit réserver la possibilité de corriger un workflow prédéfini à un administrateur ou à un utilisateur autorisé.	O
10.4.8	Si un administrateur modifie et sauvegarde un workflow, le SAE devrait archiver une copie du workflow avant modification (en indiquant en métadonnée la période d'utilisation) et devrait automatiquement attribuer un nouveau numéro de version au workflow modifié.	O
10.4.9	Le SAE ne doit pas limiter le nombre de workflows utilisables.	P
10.4.10	Le SAE doit enregistrer dans l'historique des événements toute création et toute modification de workflow prédéfini.	O
10.4.11	Le SAE devrait permettre aux utilisateurs de créer, d'utiliser et de sauvegarder des workflows à leur convenance (appelé parfois workflows ad hoc)	O
10.4.12	Le SAE devrait inclure une interface graphique pour permettre aux administrateurs et aux utilisateurs de créer, gérer et corriger des workflows.	O

Réf	Exigence	Test
10.4.13	<p>Le SAE devrait faciliter le choix du sort final, la révision et le processus d'export ou de transfert, en permettant un reporting sur :</p> <ul style="list-style-type: none"> <li>• l'état d'avancement de la révision : en attente, en progrès, détail des relecteurs et date ;</li> <li>• les documents en attente de sort final ;</li> <li>• l'état d'avancement des transferts.</li> </ul>	O
10.4.14	Si une action de révision ou de destruction vise un document ou un dossier du workflow, le SAE doit le signaler à un administrateur.	O
10.4.15	Le SAE doit garantir que tous les documents et dossiers conservent leurs liens au sein du workflow.	P
10.4.16	Le SAE devrait organiser les documents et dossiers en files d'attente contrôlables par les administrateurs.	O
10.4.17	Le SAE doit permettre aux utilisateurs de déclencher et d'utiliser des workflows définis par les administrateurs.	O
10.4.18	Le SAE doit permettre aux utilisateurs de contrôler l'avancement des workflows qu'ils ont lancés ou qui les concernent.	O
10.4.19	Le SAE devrait admettre la déclaration automatique d'un document comme une tâche au sein du workflow.	O
10.4.20	Le SAE ne devrait pas limiter le nombre de tâches dans un workflow.	P
10.4.21	Le SAE devrait pouvoir organiser des files d'attente prioritaires.	O
10.4.22	Le SAE devrait inclure une fonction de « <a href="#">rendez-vous</a> ».	O
	<i>Ceci suppose que le workflow s'interrompt pour attendre l'arrivée d'un document. A sa réception, le flux reprend automatiquement.</i>	
10.4.23	<p>Le SAE doit faciliter la définition de différents profils selon les utilisateurs du workflow.</p> <p><i>Exemples :</i></p> <ul style="list-style-type: none"> <li>• un profil d'administrateur (avec le droit de réattribuer les tâches ou les actions à un autre utilisateur ou groupe) ;</li> <li>• un superviseur (avec le droit de lancer un workflow pour gérer les anomalies dans tel ou tel cas) ;</li> <li>• les simples utilisateurs (individus et groupes).</li> <li>• Ces profils sont à distinguer des profils du SAE présentés à la section 13.4.</li> </ul>	O
10.4.24	Le SAE devrait permettre à un administrateur de fixer le nombre maximum de tâches d'un workflow au moment de la configuration.	O

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
10.4.25	Le SAE devrait permettre aux administrateurs qui créent un workflow de fixer des échéances à chaque tâche et qu'un utilisateur identifié ou un administrateur soit alerté des dépassements d'échéance.	0
10.4.26	Le SAE devrait permettre aux administrateurs qui créent un workflow de choisir dans une liste prédéfinie les actions qui incombent à chaque participant.	0
10.4.27	Le SAE devrait permettre aux administrateurs qui créent un workflow de choisir les participants : <ul style="list-style-type: none"> <li>• par nom ;</li> <li>• par profil ;</li> <li>• par service.</li> </ul>	0
10.4.28	Les administrateurs devraient pouvoir attribuer des autorisations à des utilisateurs individuels de telle sorte que ceux-ci puissent réaffecter les tâches à un autre utilisateur ou groupe.  <i>Un utilisateur peut souhaiter faire suivre un dossier ou un document à quelqu'un d'autre à cause du contenu, parce que le collègue qui devait s'en occuper est en congé, etc.</i>	0
10.4.29	Le SAE devrait permettre aux participants de visualiser les files d'attente qui les concernent puis : <ul style="list-style-type: none"> <li>• permettre aux participants choisir les tâches ;</li> </ul> ou <ul style="list-style-type: none"> <li>• afficher les tâches dans l'ordre d'arrivée ;</li> </ul> l'option étant à fixer au lancement du workflow.	0
10.4.30	Le SAE devrait permettre de conditionner le workflow aux instructions d'un utilisateur ou aux données du système.  <i>Il s'agit des flux qui font passer les documents ou les dossiers à l'un des participants sur la base d'une décision de l'un d'eux. Par exemple, un flux peut acheminer un document soit à un contrôleur financier soit à un service de consolidation des achats, selon les instructions du chef des ventes ; ou encore, le flux peut dépendre de la valeur de l'achat, calculée par le système.</i>	0
10.4.31	Le SAE devrait permettre aux utilisateurs d'interrompre temporairement un flux pour se consacrer à une autre tâche, et d'y revenir plus tard (y compris après avoir quitté le système).	0
10.4.32	Le SAE doit notifier à un utilisateur participant l'arrivée d'un dossier ou d'un document dans sa corbeille électronique.  <i>MoReq2 ne précise pas si cette corbeille correspond à la boîte de messagerie du participant ou si elle est distincte.</i>	0

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>10.4.33</b>	Le SAE devrait faciliter le suivi des dossiers et documents au travers d'une fonction de rappel (appelé aussi « pense-bête ») qui permet à un utilisateur de demander à revoir le dossier ou le document plus tard.	O
<b>10.4.34</b>	Le SAE doit fournir un mécanisme permettant à un utilisateur d'attirer l'attention d'un collègue sur tel ou tel document.  <i>Ce peut être la messagerie existante, ou un système de messagerie indépendant ou propriétaire.</i>	O
<b>10.4.35</b>	Le SAE devrait comporter la possibilité de déclencher le workflow automatiquement à réception d'un type de document donné.  <i>Exemple, le workflow pour la gestion de prêt peut être déclenché automatiquement par la réception du document « formulaire de demande de prêt ».</i>	O
<b>10.4.36</b>	Le SAE devrait permettre de réceptionner dans des répertoires spécifiques les documents électroniques déclencheurs de workflows (le workflow étant déterminé par le type de document ou d'autres métadonnées).	O
<b>10.4.37</b>	Le SAE doit fournir des fonctions de reporting complètes pour permettre aux utilisateurs autorisés et aux administrateurs de piloter le volume de tâches, les performances et les exceptions.	O
<b>10.4.38</b>	Le SAE devrait permettre de capturer et d'archiver un processus de workflow.	O
<b>10.4.39</b>	Quand un ou plusieurs dossiers ou documents ont fait l'objet de plusieurs workflows, le SAE doit permettre aux utilisateurs de préciser l'identifiant(s) et la version(s) de workflow(s) utilisés.	O
<b>10.4.40</b>	Le SAE doit garantir que les contrôles d'accès sont gérés en permanence.  <i>Autrement dit, il doit être impossible de configurer un workflow pour attribuer à un utilisateur un accès auquel il n'a pas droit par ailleurs.</i>	P
<b>10.4.41</b>	Le SAE devrait être compatible avec le modèle de référence de la Workflow Management Coalition (WfMC)	O
<b>10.4.42</b>	Le SAE devrait permettre l'export d'un processus de workflow standard ou d'une de ses composantes selon la norme XML schéma(s).	N
<b>10.4.43</b>	L'historique des événements du workflow devrait être intégré dans celui du SAE.	O
<b>10.4.44</b>	L'historique des événements du workflow doit être inaltérable.	O

## 10.5 GESTION DE DOSSIERS SÉRIELS

---

Cette section énonce les exigences concernant la gestion des « dossiers sériels » dans un SAE conforme à MoReq2. Voir le glossaire pour la définition et la description des dossiers sériels.

Un « dossier sériel » est défini dans le glossaire de MoReq2 comme un dossier traitant d'une ou plusieurs opérations réalisées, totalement ou partiellement, de manière structurée. Ici, « structuré » signifie que ces opérations suivent des règles qui sont ou pourraient être documentées, suivant un processus cohérent (les utilisateurs ne sont pas autorisés à réinventer le processus) et répétitif. Les contenus des documents d'un dossier sériel peuvent eux-mêmes être structurés (formulaires remplis en ligne par exemple) ou non structurés (messages électroniques ou scans de formulaires papier), avec différentes combinaisons possibles. La caractéristique essentielle des dossiers sériels est qu'ils procèdent de processus structurés, au moins en partie.

Les principales caractéristiques des dossiers sériels sont que :

- ils sont produits en nombre ;
- ils sont structurés ou partiellement structurés ;
- ils sont utilisés et gérés dans le cadre d'un processus défini et connu ;
- ils doivent être conservés pour des durées précises, dictées par la législation ou la réglementation ;
- ils ont un contenu et/ou une structure similaire ;
- ils ont des dates d'ouverture et de clôture connues ;
- ils peuvent être ouverts et clos par des gestionnaires de dossiers (experts, employés ou système de traitement de données) sans que cela nécessite l'approbation de leur hiérarchie.

Du fait même de leur caractère structuré, les dossiers sériels comportent généralement des sous-dossiers, paramétrés d'après un modèle. Ils peuvent aussi comporter des volumes. Voir la section 3.3 pour plus de détail sur les fonctionnalités liées aux dossiers, sériels ou non.

La gestion de dossiers sériels met fréquemment en cause une autre application métier (par exemple, traitement de demandes de licence ou un système de suivi d'enquêtes). Elle est souvent dépendante de workflows (voir les détails à la section 10.4).

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>10.5.1</b>	<p>Un administrateur doit être en mesure de configurer le SAE pour permettre au moins un profil de « gestionnaire de dossiers sériels » (voir le glossaire), avec cette spécificité que les gestionnaires de dossiers sériels peuvent avoir des autorisations d'accès différentes pour les dossiers sériels et les autres dossiers.</p> <p><i>Bien souvent les gestionnaires de dossiers sériels peuvent créer, ouvrir et clore des dossiers sériels dans le cours quotidien de leur travail mais ils n'auront pas l'autorisation de créer, d'ouvrir ou de fermer des dossiers non sériels. Pour les dossiers non sériels, ce niveau de responsabilité est réservé aux administrateurs.</i></p>	0

Réf	Exigence	Test
10.5.2	Le SAE devrait permettre un mécanisme optionnel de nommage des dossiers, configurable par l'administrateur, avec des noms (noms de personnes...) et/ou des dates (date de naissance...) ou un identifiant unique de dossier comme intitulé du dossier, issus de listes extérieures et validés automatiquement.	0
10.5.3	Les métadonnées utilisées pour le nommage automatique des dossiers (cf. 10.5.2) doivent être obligatoires ou du moins des valeurs par défaut devraient être fournies lors de la définition du processus de nommage. Si les métadonnées de base (tels que noms et dates), utilisées pour créer le titre du dossier, sont modifiées, le SAE ne doit pas automatiquement mettre à jour le titre du dossier.	0
10.5.4	Les règles de nommage automatique des dossiers (cf. 10.5.2) devraient être paramétrables de différentes façons pour des séries différentes du plan de classement.  <i>Les trois exigences ci-dessus conviennent aux dossiers sériels. Toute liste utilisée pour la validation peut être gérée par le SAE ou à l'extérieur.</i>  <i>Lorsqu'un titre de dossier a été créé automatiquement par un mécanisme de concaténation de métadonnées tels que noms de personne, date de naissance, etc., il est possible de mettre à jour ces métadonnées originales sur lesquelles s'appuie le titre : changement du nom de personne, erreur de saisie de la date... Dans ce cas, le titre du dossier tiré de ces métadonnées ne devrait pas être automatiquement modifié dans la mesure où il a peut-être déjà été utilisé (dans un courrier, ou enregistré dans un système). En dehors de l'interdiction de modifier automatiquement un titre de dossier, MoReq2 n'a pas d'autres exigences sur les opérations possibles.</i>  <i>Différentes opérations sont possibles, notamment :</i> <ul style="list-style-type: none"> <li>• ignorer les modifications de métadonnées ; le titre du dossier ne change pas ;</li> <li>• alerter un administrateur des modifications, lequel peut éventuellement mettre à jour le titre du dossier ;</li> <li>• avertir l'utilisateur qui effectue les modifications que les métadonnées sont utilisées dans le titre et lui demander de confirmer ses modifications ;</li> <li>• empêcher l'utilisateur de mettre à jour les métadonnées et l'inviter à faire suivre les changements souhaités à un administrateur ayant la main pour changer ces métadonnées.</li> </ul>	0
10.5.5	Le SAE doit permettre la création de dossiers sériels par tout utilisateur ayant un profil de gestionnaire de dossiers.	0
10.5.6	Le SAE doit permettre aux utilisateurs d'accéder à un dossier sériel et de l'ouvrir en saisissant son identifiant de dossier sériel.  <i>Le plus souvent l'identifiant d'un dossier sériel (un titre ou un numéro) est fourni par un système externe. Une interface devrait aider l'utilisateur à valider un identifiant saisi manuellement. Celui-ci est différent, et s'ajoute à l'identifiant système et au code de classement.</i>	0

Réf	Exigence	Test
10.5.7	<p>Le SAE doit fournir une API (interface de programmation) ou l'équivalent pour faciliter l'intégration avec les autres applications métier. Les fonctionnalités à prendre en compte sont au minimum :</p> <ul style="list-style-type: none"> <li>• l'autre application métier crée, ouvre et clos des dossiers sériels dans le SAE ;</li> <li>• l'autre application métier produit les titres des dossiers sériels ;</li> <li>• le code de classement d'un dossier sériel nouvellement créé est transféré vers une autre application métier ;</li> <li>• l'autre application métier transfère les documents à archiver dans les dossiers sériels du SAE ;</li> <li>• l'autre application métier exécute les règles de conservation/destruction visant les dossiers clos ;</li> <li>• une gestion des erreurs est prévue si le système lance une action invalidée par un autre système.</li> </ul> <p><i>C'est comme si l'application métier agissait à la place d'un utilisateur - le SAE ne devrait pas faire la différence entre les deux.</i></p> <p><i>MoReq2 ne précise pas la nature des traitements d'erreur. Toutefois, les deux exigences suivantes donnent des pistes.</i></p>	P
10.5.8	<p>S'il reçoit d'une application métier externe une requête apparemment invalide, le SAE doit éviter :</p> <ul style="list-style-type: none"> <li>• de poursuivre une action invalide ;</li> <li>• de conduire à une faille logicielle du SAE ou de l'application externe.</li> </ul>	O
10.5.9	<p>S'il reçoit d'une application métier externe une requête apparemment invalide, le SAE doit alerter un utilisateur autorisé pour qu'il apporte une action corrective.</p>	O
10.5.10	<p>Quand le SAE s'interface avec une autre application métier, il faut qu'un administrateur puisse limiter les actions de l'autre application à certaines séries du plan de classement du SAE.</p> <p><i>Autrement dit, une application externe ne doit en aucun cas déclencher une action qui affecterait des séries, des dossiers ou des documents en dehors des dossiers sériels.</i></p>	O
10.5.11	<p>Quand le SAE s'interface avec une autre application métier, il faudrait qu'un utilisateur puisse accéder facilement aux dossiers des deux applications.</p> <p><i>Autrement dit, un utilisateur qui a utilisé les fonctions de l'autre application métier pour localiser ou identifier une affaire ou un dossier (par exemple à l'aide des fonctions de recherche d'une adresse postale) doit pouvoir ouvrir ce dossier dans le SAE facilement, sans avoir à ressaisir l'identifiant du dossier. Pareillement, un utilisateur qui a ouvert un dossier sériel dans le SAE (en naviguant dans le plan de classement, en faisant une requête ou autrement) doit pouvoir se connecter à l'écran correspondant dans l'autre application de la même façon.</i></p>	N

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>10.5.12</b>	Si le SAE permet qu'une autre application métier crée de nouveaux dossiers sériels, il doit être en mesure de recevoir de cette application les métadonnées des dossiers.	0
<b>10.5.13</b>	Le SAE doit permettre de paramétrer les dossiers sériels avec des métadonnées qui leur sont propres.  <i>Un dossier sériel peut ainsi nécessiter une ou plusieurs métadonnées de type « statut » ou « progrès ».</i>	0
<b>10.5.14</b>	Le SAE doit permettre aux utilisateurs de rechercher des dossiers sériels, de les archiver et d'effectuer toutes les actions valides, en utilisant l'identifiant du dossier sériel au lieu du code de classement.  <i>La plupart des dossiers sériels sont identifiés par un identifiant de dossier unique du type numéro comptable ou numéro de plainte. Les utilisateurs doivent pouvoir travailler sur ces dossiers en indiquant simplement cet identifiant, et sans recourir au code de classement du SAE (bien que l'utilisation de ce code reste possible).</i>	P
<b>10.5.15</b>	<i>Si le SAE reçoit des documents à contenu structuré provenant d'une autre application métier, il devrait pouvoir extraire automatiquement les métadonnées de ces documents.</i>	0
<b>10.5.16</b>	Si le SAE reçoit des documents à contenu structuré provenant d'une autre application métier, il devrait pouvoir utiliser cette extraction de métadonnées pour archiver les documents dans le bon dossier.  <i>Par exemple, si un SAE reçoit un formulaire électronique de déclaration de plainte d'une application de gestion des plaintes, il devrait pouvoir en extraire l'identifiant du plaignant et le type de formulaire, et utiliser ces données pour classer les documents dans le bon dossier (grâce au numéro de plaignant) et dans le bon sous-dossier (grâce au type de formulaire).</i>	0
<b>10.5.17</b>	Le SAE doit garantir que toutes les opérations effectuées sur une série, un dossier ou un document, par un utilisateur autorisé ou par une autre application métier, sont tracées dans l'historique des événements.	0
<b>10.5.18</b>	Le SAE doit pouvoir produire des statistiques sur toutes les opérations effectuées sur tout dossier, que ce soit par un utilisateur autorisé ou par un autre système.	0

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
10.5.19	<p>Le SAE doit pouvoir fournir aux administrateurs des statistiques montrant au minimum :</p> <ul style="list-style-type: none"><li>• le nombre de documents archivés automatiquement dans des dossiers sériels à partir d'autres applications métiers pour telle période ;</li><li>• le nombre de documents archivés manuellement dans des dossiers sériels pour telle période ;</li><li>• le nombre de dossiers sériels ouverts et clos automatiquement par d'autres applications métiers pour telle période ;</li><li>• le nombre de dossiers sériels ouverts et clos manuellement pour telle période.</li></ul>	0

## 10.6 INTEGRATION AVEC LES SYSTEMES DE GESTION DE CONTENU

---

Cette section traite des exigences relatives à l'intégration des « [systèmes de gestion de contenu](#) » (CMS) avec les SAE. Les systèmes de gestion de contenu incluent aujourd'hui la plupart des fonctionnalités de GED (voir section 10.3). Les pages qui suivent visent plus particulièrement les exigences fonctionnelles intéressant un SAE et ne décrivent pas toutes les fonctionnalités de la gestion de contenu ou de la GED ; les fonctionnalités exposées ne suffisent pas à faire d'un SAE un outil de gestion de contenu à part entière.

Les CMS incluent et étendent les fonctionnalités de GED à tous types d'informations (contenu) et au-delà de l'archivage. Les CMS répondent à d'autres aspects de gestion de l'information que les SAE. Les points communs sont :

- publier l'information, sur des sites ou des portails, parfois sur plusieurs canaux avec différents types de conversion de fichier ;
- gérer l'information en provenance de plusieurs sources ;
- reformater l'information et/ou la migrer avec différents modes de conversion ;
- relier différentes versions, conversions et traductions de documents ;
- gérer les composants des documents.

A ce jour, l'utilisation ou le besoin d'intégration le plus courant d'un CMS pour un SAE concerne principalement la publication web. Ce point est abordé mais la section vise aussi d'autres formes de gestion de contenu.

Les fonctionnalités de gestion de contenu peuvent être fournies par un CMS séparé du SAE ou par une solution intégrée qui offre conjointement les fonctionnalités de gestion de contenu et d'archivage électronique. Pour plus de clarté, les exigences de MoReq2 décrites ici les considèrent séparément mais cette séparation n'est pas en soi une exigence.

La figure 10.1 montre, de manière volontairement simplifiée, la relation entre un SAE et un CMS :

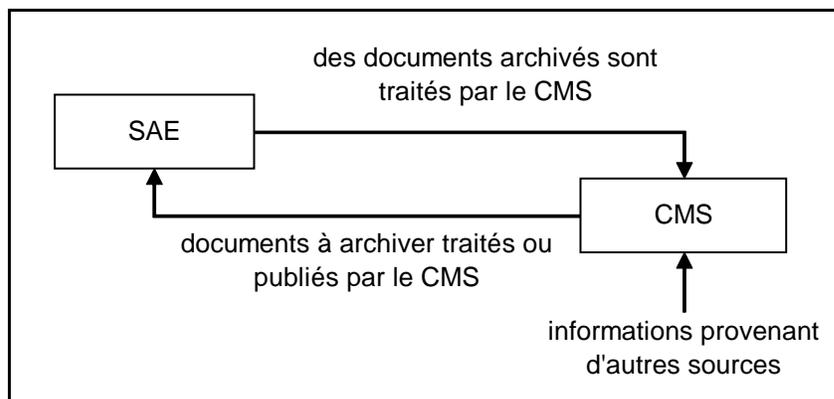


Figure 10.1

Ce schéma met en évidence que :

- Des copies de documents archivés peuvent passer du SAE au CMS pour traitement (en général mise en forme, préparation de différentes conversions, publication).
- Des documents issus du CMS peuvent être envoyés au SAE pour capture et archivage, ce qui peut intervenir pendant le traitement au sein du CMS ou après publication. Les documents archivés peuvent comporter des pages web, des sites web, de nouvelles conversions des documents déjà archivés.
- Le CMS peut également recevoir des informations d'autres sources, de sorte que les documents envoyés pour archivage au SAE peuvent combiner des informations provenant du SAE et des informations exogènes.

A noter que l'envoi vers le SAE peut prendre plusieurs formes :

- une copie du document est transférée d'une application à l'autre ;
- les documents archivés sont stockés dans un entrepôt commun au CMS et au SAE et seuls des messages d'identification des documents à archiver ou archivés circulent entre les applications ;
- les documents archivés sont stockés dans un entrepôt commun au CMS et au SAE et les deux applications s'y réfèrent sans avoir besoin d'échanger d'information.

Dans la suite du texte, l'expression « l'envoi de copie » renvoie à l'une de ces possibilités (voire d'autres).

Les technologies de gestion de contenu évoluent rapidement et les entreprises/organisations qui recherchent cette intégration doivent bien préciser leurs besoins, car ces exigences sont sans doute insuffisantes ; elles constituent toutefois un point de départ pour une analyse plus approfondie.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
10.6.1	<p>Le SAE doit être en mesure de réceptionner les documents provenant du CMS, avec leurs métadonnées et doit :</p> <ul style="list-style-type: none"> <li>• capturer et archiver automatiquement le document dans le bon dossier, grâce aux métadonnées ;</li> </ul> <p>ou</p> <ul style="list-style-type: none"> <li>• demander à un utilisateur d'indiquer le dossier correspondant.</li> </ul>	0

Réf	Exigence	Test
10.6.2	<p>Le SAE doit être en mesure de capturer et d'archiver les composants et les types de fichiers spécifiques du CMS, notamment :</p> <ul style="list-style-type: none"> <li>• les logs de gestion de contenu ;</li> <li>• les feuilles de style.</li> </ul>	O
10.6.3	<p>Le SAE doit gérer les métadonnées du CMS en plus des métadonnées d'archivage requises par MoReq2.</p> <p><i>Un CMS peut utiliser des métadonnées spécifiques à la gestion de contenu telles que :</i></p> <ul style="list-style-type: none"> <li>• <i>adresse IP ;</i></li> <li>• <i>statut ;</i></li> <li>• <i>langue ;</i></li> <li>• <i>date de publication ;</i></li> <li>• <i>date effective ;</i></li> <li>• <i>motif de modification.</i></li> </ul> <p><i>Le SAE doit pouvoir stocker ces données, même si elles ne servent pas à l'archivage. Il n'est pas nécessaire que le SAE stocke toutes les métadonnées créées ou utilisées par le CMS ; les éléments à conserver seront définis au moment de la configuration sur la base des besoins métier.</i></p> <p><i>Cette exigence est particulièrement importante. Elle permet qu'un ensemble très varié d'informations produites par le CMS soit ensuite stocké dans le SAE sous forme de métadonnées.</i></p>	O
10.6.4	<p>Lorsqu'un document transféré du CMS vers le SAE pour capture et archivage est lié à un document déjà archivé dans le SAE (par exemple, une conversion de fichier différente ou une traduction), le SAE ne doit pas supprimer ou modifier le document préalablement archivé ; il doit archiver et stocker le nouveau document.</p>	P
10.6.5	<p>Lorsqu'un document lié à un document déjà archivé (cf. 10.6.4) est transféré du CMS vers le SAE pour capture et archivage, le SAE doit automatiquement créer un lien entre les deux (cf. 3.4.23).</p> <p><i>Ce ne sera possible que si le CMS renvoie également l'identifiant du document d'origine dans les métadonnées du nouveau document. Si ce n'est pas la cas, le SAE ne pourra passer le test de conformité à MoReq2.</i></p>	O
10.6.6	<p>Lorsqu'un document lié à un document déjà archivé (cf. 10.6.4) est transféré du CMS vers le SAE pour capture et archivage, le SAE devrait comparer les métadonnées du nouveau document avec celles du document initial pour s'assurer, autant que possible, de leur similitude ; les différences devant se limiter à l'enregistrement des modifications et actions du CMS.</p>	N
10.6.7	<p>Si les documents transférés du CMS vers le SAE se présentent sous la forme de pages web, le SAE devrait pouvoir capturer une page web ou un jeu de pages web et les archiver comme un seul document.</p>	O

Réf	Exigence	Test
	<p>La possibilité de capturer un jeu de pages web comme un seul document peut être intéressante, notamment pour stocker des photos périodiques d'un site web.</p> <p>La capture de pages web pourra nécessiter de modifier les références (hyperliens entre les pages et avec d'autres pages, références à des composants graphiques ou autres) si on veut garantir une présentation correcte des pages et conserver autant que possible leur fonction d'origine. C'est inévitable si des pages web comportant des éléments graphiques, des feuilles de style, des hyperliens, etc. doivent être conservées dans leur format d'origine sans perdre leur caractère fonctionnel ni leur fidélité. L'essentiel est que le contenu informationnel de la page web ne soit pas modifié. Voir les exigences 6.1.5 et 6.1.6.</p>	
10.6.8	Quand des documents sont reçus par le SAE en provenance du CMS, cela doit être automatiquement tracé dans l'historique des événements et dans les métadonnées des documents archivés.	0
10.6.9	Lorsqu'un utilisateur sélectionne des documents du SAE pour les envoyer au CMS, il doit pouvoir utiliser toutes les métadonnées de gestion de contenu disponibles.  <i>Pour poursuivre l'exemple de 10.6.3, l'utilisateur pourra sélectionner les documents d'une série donnée avec les valeurs « date effective » et « statut ».</i>	0
10.6.10	Le SAE devrait permettre aux utilisateurs d'effectuer des transferts de documents du SAE vers le CMS, avec les métadonnées correspondantes.  <i>Les métadonnées à transférer sont définies au moment de la configuration.</i>	0
10.6.11	Quand des documents sont transférés du SAE vers le CMS, cela doit être automatiquement tracé dans l'historique des événements et dans les métadonnées du document.	0

## 10.7 SIGNATURE ELECTRONIQUE

---

La signature électronique (parfois appelée signature numérique) consiste en une information qui est attachée ou logiquement reliée à une autre information, par exemple un document électronique à archiver, et qui sert de moyen d'authentification. La signature électronique se présente sous la forme d'une séquence de caractères. Elle utilise des algorithmes sécurisés, des procédures et des « clés » (un longue suite de caractères similaire à un mot de passe) pour attester de l'intégrité d'un document et/ou authentifier l'expéditeur ou la provenance d'un document. La signature électronique ne devrait pas être confondue avec une image bitmap ou un scan de la signature manuscrite sur papier, laquelle n'est pas sûre et ne saurait apporter aucune preuve de l'authenticité d'un document.

Une signature électronique, au sens de MoReq2, est une forme de « signature électronique avancée » telle que l'a définie la directive européenne 1999/93/EC pour un « cadre communautaire pour la signature

électronique ». Une signature électronique avancée telle que définie dans la directive, est une signature qui est :

- liée de manière unique au signataire ;
- à même d'identifier le signataire ;
- créée par des moyens que le signataire est en mesure de maintenir sous son seul contrôle ;
- liée aux données (au document) auxquelles elle se rapporte de telle manière que tout changement ultérieur des données (du document) est détectable.

Un autre cadre normatif pour la signature électronique est donné par X.509 (voir annexe 7).

Les algorithmes de signature électronique les plus largement reconnus sont, entre autres, le DSA (Digital Signature Algorithm) défini dans FIPS 186-2 (voir annexe 7) et le RSA/SHA-1.

La messagerie électronique est devenue le moyen de communication par défaut de nombreuses entreprises/organisations et cela a contribué à la dispersion de documents, archivables ou non, dans des environnements qui ne sont pas toujours contrôlés. L'utilisation de la signature électronique pour authentifier et assurer l'intégrité est en passe d'être généralisée, particulièrement dans les échanges contractuels.

Les exigences ci-après ne s'appliquent que lorsqu'il y a besoin de gérer des documents signés électroniquement. A ce jour, la signature électronique est encore sujette à des évolutions avec des incertitudes occasionnées par les périodes de test des nouvelles infrastructures et algorithmes. Cet état de fait est susceptible de durer. Les utilisateurs de MoReq2 devront donc valider ces exigences et leurs implications pour la conservation à long terme auprès des autorités compétentes.

La section ne fait pas mention des législations nationales en matière de signature électronique. Il se trouve que certaines lois exigent la conservation intégrale d'une signature pour être probante, tandis que d'autres exigent seulement la conservation des métadonnées de signature. Le cas échéant, cette question sera abordée dans le chapitre zéro réservé à chaque pays.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>10.7.1</b>	<p>Le SAE doit pouvoir capturer, vérifier (le cas échéant) et stocker, au moment de l'archivage, les signatures électroniques, les certificats associés et les coordonnées des prestataires de certification.</p> <p><i>C'est d'autant plus essentiel que ces informations ne pourront pas être recréées ultérieurement.</i></p>	O
<b>10.7.2</b>	<p>Le SAE doit permettre aux administrateurs de paramétrer le système, initialement ou plus tard, afin de stocker les métadonnées de vérification des documents signés électroniquement (clés publiques incluses). Il convient de capturer avec le document, au moment de l'archivage, une de ces trois informations :</p> <ul style="list-style-type: none"><li>• le fait que la vérification s'est opérée avec succès ;</li><li>• l'information décrivant le processus de vérification ;</li><li>• toutes les données de vérification.</li></ul> <p><i>C'est d'autant plus essentiel que ces informations ne pourront pas être recréées ultérieurement.</i></p>	O

Réf	Exigence	Test
10.7.3	<p>Le SAE devrait avoir une interface normalisée pour intégrer au fur et à mesure les nouvelles technologies de signature électronique.</p> <p><i>Exemple de norme : le XML Dey Management Spec (XKMS, voir annexe 7).</i></p> <p><i>C'est particulièrement important compte tenu des évolutions dans ce domaine.</i></p>	N
10.7.4	<p>Le SAE devrait pouvoir vérifier la validité d'une signature électronique, y compris le certificat associé en le rapprochant au moment de la capture de la liste des révocations de certificats électroniques, et stocker la réponse dans les métadonnées du document archivé. Toute vérification négative devrait être signalée à un utilisateur dédié ou à un administrateur.</p> <p><i>C'est d'autant plus important que cette vérification ne pourra pas être effectuée ultérieurement.</i></p>	O
10.7.5	<p>Lors de la capture d'un message électronique, le SAE doit pouvoir capturer automatiquement et conserver comme métadonnées les détails du processus de vérification de la signature, à savoir :</p> <ul style="list-style-type: none"> <li>• le fait que la validité de la signature a été vérifiée ;</li> <li>• l'identité de l'individu qui a effectué la vérification (le cas échéant) ;</li> <li>• l'émetteur du certificat ;</li> <li>• le numéro de série du certificat électronique associé à la signature ;</li> <li>• le prestataire de certification auprès de qui la signature a été validée ;</li> <li>• la date et l'heure de la vérification.</li> </ul> <p><i>C'est d'autant plus essentiel que ces informations ne pourront pas être recréées ultérieurement. Du fait des changements de logiciel, de l'expiration des certificats, du défaut de pérennité des autorités extérieures, il est impossible de garantir une vérification des signatures électroniques sur de longues périodes. Raison de plus pour tracer que la signature a été vérifiée avec succès.</i></p>	O
10.7.6	<p>Le SAE devrait comporter une fonction permettant de démontrer l'intégrité des documents signés électroniquement.</p> <p><i>La vérification d'une signature électronique en est un bon exemple. Cette démonstration d'intégrité devrait fonctionner même si un administrateur a effectué des modifications autorisées sur les métadonnées du document archivé.</i></p> <p><i>La façon de procéder n'est pas indiquée.</i></p>	N
10.7.7	<p>Le SAE devrait pouvoir stocker avec le document électronique :</p> <ul style="list-style-type: none"> <li>• la signature électronique associée ;</li> <li>• le certificat électronique de vérification de la signature.</li> </ul>	O
10.7.8	<p>L'administrateur du SAE devrait pouvoir décider si le SAE doit stocker le ticket de validation renvoyé par le système qui vérifie la signature.</p>	O

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
	<i>Le ticket de validation est parfois appelé jeton.</i>	
<b>10.7.9</b>	Le SAE devrait permettre à un administrateur d'apposer une signature électronique à un dossier, à un document ou à un message pendant un processus d'export ou de transfert de sorte que l'intégrité et la source du dossier, du document ou du message de transfert puissent être ultérieurement vérifiées.  <i>Un message de transfert est un message envoyé d'une application vers une autre dans le cadre du protocole utilisé pour les transferts entre systèmes.</i>	0
<b>10.7.10</b>	Une signature électronique apposée pendant un export ou un transfert (cf. 10.7.9) devrait recevoir une validation externe, de sorte que l'intégrité et la source du dossier, du document ou du message puissent être ultérieurement vérifiées.  <i>Pour ce faire, le SAE doit pouvoir exporter, avec le document, un certificat électronique avec la clé publique de l'entreprise/organisation.</i>	0

## 10.8 CHIFFREMENT

---

Le chiffrement est un processus qui consiste en une transformation complexe d'un objet électronique de telle sorte qu'aucune application ne puisse le restituer de manière lisible ou intelligible sans application du processus inverse de déchiffrement. Ce processus sert à sécuriser les objets électroniques, par une transformation qui exige l'utilisation de codes électroniques sécurisés.

Les exigences ci-après ne s'appliquent que lorsqu'il y a besoin de gérer des documents chiffrés.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>10.8.1</b>	Lors de l'expédition ou de la réception d'un document électronique chiffré par une application interfacée avec le SAE, celui-ci doit pouvoir en restreindre l'accès aux seuls utilisateurs identifiés comme détenteurs de la clé de déchiffrement correspondante, en sus des autres contrôles d'accès attribués à ce document.	0
<b>10.8.2</b>	Le SAE doit pouvoir capturer et stocker, dès la capture, l'information de chiffrement et les coordonnées des autorités de vérification.	0

Réf	Exigence	Test
10.8.3	<p>Lors de la transmission d'un document électronique chiffré par une application interfacée avec le SAE, le SAE devrait pouvoir conserver comme métadonnées de ce document :</p> <ul style="list-style-type: none"> <li>• le fait même d'une transmission chiffrée ;</li> <li>• le numéro de série du certificat électronique (s'il y a lieu) ;</li> <li>• le type d'algorithme ;</li> <li>• le niveau de chiffrement ;</li> <li>• la date et l'heure du chiffrement et/ou du déchiffrement, le cas échéant.</li> </ul>	O
10.8.4	Le SAE devrait pouvoir assurer la capture de documents chiffrés directement à partir d'une application qui possède une fonction de chiffrement.	O
10.8.5	<p>Le SAE devrait permettre de déchiffrer le document lors de l'import ou de la capture. Cette fonction serait paramétrée par un administrateur au démarrage ou plus tard.</p> <p><i>Cette fonction peut être souhaitable en cas d'archivage de forts volumes à durée de conservation longue (dans la mesure où le chiffrement restreint la possibilité de relire les documents sur le long terme). Dans ce cas, l'entreprise/organisation s'appuiera sur l'historique des événements ou l'équivalent pour prouver que le document a bien été chiffré avant d'être déchiffré. Ailleurs, d'un point de vue légal, cette fonction sera écartée. Pour plus de détail sur les transferts et les imports, voir les sections 5.3 et 3.1.</i></p>	O
10.8.6	Le SAE devrait avoir une structure permettant d'intégrer les nouvelles technologies de chiffrement.	N

## 10.9 GESTION DES DROITS NUMERIQUES

---

Ce module optionnel ne comporte aucune exigence testable dans la forme actuelle. Comme il est précisé plus loin, les tests n'auront de sens que si les exigences sont adaptées à des technologies spécifiques.

La gestion des droits numériques (DRM) et la gestion des droits numériques en entreprise (E-DRM) font référence à un ensemble de technologies non encore normalisées, visant à protéger la propriété intellectuelle et/ou à restreindre la diffusion de l'information. Les DRM sont généralement associés à la protection de la propriété intellectuelle (notamment dans le monde musical, pour l'édition électronique et l'industrie du film), alors que les E-DRM renvoient à la mise en œuvre de restrictions dans la diffusion de l'information métier, pour des raisons de sécurité ou de confidentialité commerciale. Les frontières ne sont cependant pas étanches et les deux peuvent se rencontrer dans le contexte d'un SAE. C'est pourquoi, on parlera dans la suite de technologies de DRM - E-DRM.

Exemples de DRM - E-DRM :

- Tatouage électronique (dit aussi tatouage numérique) qui embarque une information de propriété intellectuelle visible dans le document électronique. Le procédé de fixation de l'information est complexe, ce qui rend son effacement difficile.
- Stéganographie, qui applique également une information de propriété intellectuelle mais de manière invisible ou, pour un fichier audio, inaudible. La lecture de l'information de propriété intellectuelle requiert un logiciel spécial.
- Des systèmes de protection anti-copie, avec toute une variété de dispositifs.
- Un dispositif inséré dans les documents et qui permet de les voir à l'écran mais pas de les imprimer.
- Un dispositif temporaire inséré dans les documents et qui interdit leur restitution après une certaine date.

Les technologies de DRM - E-DRM sont encore émergentes. Elles sont susceptibles d'évoluer de manière significative pendant la durée de vie de MoReq2.

Ces technologies, entre autres, peuvent s'appliquer aux documents archivés sous de nombreux formats, y compris le son et le film numériques.

Ces technologies constituent un défi particulier pour l'archivage dans la mesure où elles restreignent ou même rendent impossible la restitution des documents archivés. Exemples :

- Certains types de filigranes dépendent de la présence d'un module d'extension (plug-in) pour une visualisation complète. Certes, le document archivé comportant un filigrane peut être visualisé sans l'extension mais l'information complète sur ce filigrane ne pourra être obtenue sans l'extension. Or, plus le temps passe et plus l'extension risque d'être indisponible.
- Un message électronique contient une caractéristique temporaire qui en interdit la lecture après une date donnée. Ce problème est d'autant plus insidieux qu'il n'est pas forcément apparent au moment de la capture.

Les utilisateurs et administrateurs responsables de l'archivage des documents électroniques devraient avoir un minimum de connaissances sur l'impact de la DRM - E-DRM sur le SAE. Par ailleurs, les conséquences de ces technologies sur l'archivage peuvent être minimisées si les dispositifs de DRM - E-DRM sont retirés des documents au moment de leur capture. Il s'agit toutefois dans les deux cas de questions d'organisation qui dépassent le cadre de MoReq2.

Les technologies en cause sont très variées et leurs effets sur les documents archivés également. On ne saurait donc énoncer des exigences générales pertinentes applicables à toutes les technologies. Cette section formule toutefois quelques exigences génériques qui seront développées par les utilisateurs de MoReq2 en cas de cahier des charges ou d'acquisition dans ce domaine. Par exemple, si des dispositifs temporaires sont prévus, les exigences devront être adaptées et précisées pour les prendre en compte.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
10.9.1	Le SAE doit être capable de capturer et de conserver des documents comportant des dispositifs de DRM - E-DRM.	N

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
10.9.2	<p>Le SAE devrait pouvoir identifier la présence de dispositifs de DRM - E-DRM à la capture d'un document. Si un dispositif de ce type est repéré, le SAE devrait en informer l'utilisateur et fournir l'une des options suivantes :</p> <ul style="list-style-type: none"> <li>• conserver le dispositif de DRM - E-DRM ;</li> <li>• retirer le dispositif de DRM - E-DRM, si c'est possible ;</li> <li>• suspendre le processus de capture.</li> </ul>	N
10.9.3	<p>Le SAE devrait pouvoir retirer le dispositif de DRM - E-DRM pendant la capture du document.</p> <p><i>On peut l'exiger dans certains cas mais l'exigence ne peut être généralisée car cela nécessiterait un contournement arbitraire des fonctions de sécurité. Si le dispositif de DRM - E-DRM est retiré, cela doit être tracé dans l'historique des événements.</i></p>	N
10.9.4	<p>Le SAE devrait inclure la possibilité de contrôler les accès aux documents archivés sur la base des restrictions de propriété intellectuelle et de produire des données de suivi des accès.</p> <p><i>Cette courte assertion couvre un grand nombre de fonctionnalités qui dépassent le cadre de MoReq2. Cette exigence peut être satisfaite par la mise en place d'un lien vers une application séparée.</i></p>	N
10.9.5	<p>Le SAE doit être capable de restituer correctement les documents archivés avec des dispositifs de DRM - E-DRM, dans la limite de ce qui est autorisé.</p>	N
10.9.6	<p>Le SAE doit être capable de repérer et de stocker lors de la déclaration les informations inscrites dans le dispositif de DRM - E-DRM, dans la limite de ce qui est autorisé.</p> <p><i>Par exemple, les identités des détenteurs des droits de propriété intellectuelle, codées dans le filigrane ; ou une date d'expiration.</i></p> <p><i>On peut l'exiger dans certains cas mais l'exigence ne peut être généralisée car cela nécessiterait un contournement arbitraire des fonctions de sécurité.</i></p>	N
10.9.7	<p>Le SAE devrait permettre l'introduction de nouvelles technologies de DRM - E-DRM.</p>	N
10.9.8	<p>Le SAE devrait être capable de mettre en œuvre des dispositifs de DRM - E-DRM pendant l'export.</p> <p><i>C'est particulièrement souhaitable si le dispositif de DRM - E-DRM a été retiré.</i></p>	N

## 10.10 SYSTEMES DISTRIBUES

---

Cette section regroupe les exigences pour les entreprises/organisations qui ont besoin d'un SAE multi-sites.

De nombreuses entreprises/organisations possèdent plusieurs sites d'activité. Lorsque ces sites sont relativement proches les uns des autres, ou si les connexions réseau entre les sites sont bonnes (capacité suffisante), un seul SAE peut suffire pour les besoins de l'ensemble. Dans ce cas, tous les sites fonctionnent comme s'ils étaient regroupés et les exigences qui suivent ne s'appliquent pas. Toutefois, lorsque les sites sont géographiquement éloignés ou que la connectivité n'est pas bonne, il peut être nécessaire de mettre en œuvre un SAE distribué ; les exigences de la section sont alors applicables.

Il existe plusieurs types d'architecture possibles pour les systèmes distribués. On peut avoir : un SAE qui contrôle plusieurs entrepôts de données ; plusieurs SAE ayant chacun leur(s) entrepôt(s) et communiquant entre eux ; ou d'autres approches. MoReq2 ne se prononce pas sur l'architecture ; il indique seulement les exigences essentielles pour les environnements distribués, l'expression « SAE distribué » ne préjugant pas de l'architecture.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>10.10.1</b>	Le SAE doit pouvoir être configuré par un administrateur pour une utilisation partagée entre plusieurs sites.	N
<b>10.10.2</b>	Le SAE devrait faciliter l'utilisation d'un plan de classement distribué entre plusieurs entrepôts de documents archivés électroniquement.	O
<b>10.10.3</b>	Le SAE devrait permettre à un administrateur d'assurer la maintenance des séries, dossiers, sous-dossiers, volumes et documents, avec leurs métadonnées et les historiques des événements au travers du SAE distribué de sorte que toute mise à jour soit répercutée immédiatement sur l'ensemble du système.  <i>La maintenance renvoie aux actions décrites notamment au chapitre 3 et à la section 9.1.</i>	P
<b>10.10.4</b>	Lorsque le SAE gère plusieurs entrepôts, il devrait permettre à un administrateur de préciser lequel stocke l'original de chaque série (avec les séries filles et les documents rattachés).  <i>Exemple : une entreprise/organisation peut décider de mettre en place un entrepôt par site, chaque entrepôt devant stocker les documents archivés sur ce site (sous réserve que la conception du plan de classement supporte cette configuration).</i>	O
<b>10.10.5</b>	Lorsque le SAE gère plusieurs entrepôts, il devrait permettre à un administrateur de préciser le(s)quel(s) stocke(nt) automatiquement la copie de chaque série (avec les séries filles et les documents rattachés).	O

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
	<p><i>Exemple : une entreprise/organisation peut décider que :</i></p> <ul style="list-style-type: none"> <li>• <i>tous les entrepôts sont recopiés dans l'entrepôt du siège ;</i></li> <li>• <i>dans un territoire donné, tous les entrepôts doivent être recopiés entre eux.</i></li> </ul> <p><i>Cela suppose, bien sûr, que les entrepôts soient systématiquement synchronisés. Sont concernés :</i></p> <ul style="list-style-type: none"> <li>• <i>les documents archivés ;</i></li> <li>• <i>les métadonnées.</i></li> </ul>	
10.10.6	<p>Lorsque le SAE gère plusieurs entrepôts, il devrait permettre à un administrateur de préciser au(x)quel(s) les utilisateurs de chaque site peuvent accéder.</p> <p><i>Exemple : une entreprise/organisation peut décider que :</i></p> <ul style="list-style-type: none"> <li>• <i>les utilisateurs ne peuvent accéder qu'à l'entrepôt de leur site ;</i></li> <li>• <i>les utilisateurs peuvent accéder à l'entrepôt de leur site et à l'entrepôt du siège ;</i></li> <li>• <i>les utilisateurs du siège peuvent accéder à tous les entrepôts tandis que les utilisateurs des sites ne peuvent accéder qu'à l'entrepôt de leur site ;</i></li> <li>• <i>les utilisateurs peuvent accéder à tous les entrepôts sur leur territoire (selon une liste d'entrepôts préétablie ; cela n'implique pas que le SAE reconnaisse la notion de « territoire »).</i></li> </ul>	O
10.10.7	<p>Lorsque le SAE gère plusieurs entrepôts, il devrait permettre à un administrateur de préciser que tous les historiques des événements seront recopiés dans un seul entrepôt.</p>	O
10.10.8	<p>Le SAE doit empêcher et sinon résoudre tout problème dû à des modifications sur les sites.</p> <p><i>Par exemple, un problème peut survenir si deux administrateurs de deux sites différents effectuent des modifications distinctes sur la même série stockée dans un troisième site.</i></p>	P
10.10.9	<p>Le SAE doit permettre à un administrateur de contrôler à la fois l'ensemble du SAE distribué comme une seule entité, et chaque entrepôt individuel avec les fonctions indiquées à la section 9.2.</p>	O
10.10.10	<p>Le SAE devrait être capable de produire des rapports statistiques (voir 9.2) sur plusieurs entrepôts.</p>	O
10.10.11	<p>Le SAE devrait pouvoir mettre en mémoire cache les dossiers, sous-dossiers, volumes et documents fréquemment ou récemment consultés sur des sites utilisant des entrepôts séparés.</p>	O

Réf	Exigence	Test
	<i>Les deux exigences qui suivent ont trait à la performance du SAE distribué. Elles utilisent les expressions entre crochets (ex : &lt;xx minutes/heures&gt; selon l'explication donnée en tête du chapitre 11).</i>	
10.10.12	Lorsque le SAE a des entrepôts synchronisés, ils doivent être synchronisés dans les <xx minutes/heures> après une modification (en fonction de la disponibilité du réseau).	N
10.10.13	Le SAE doit être capable de répercuter toute modification administrative sur tous les entrepôts dans les <xx minutes/heures>.	N
	<i>Les exigences 10.10.12 et 10.10.13 ne sont que des exemples. MoReq2 n'indique pas les temps de réponse car ils dépendent des systèmes. Voir plus de détail au point 11.2.</i>	
	<i>Il est essentiel que l'architecture du système permette des temps de réponse acceptables pour tous les sites. Les utilisateurs de MoReq2 considéreront séparément les temps de réponse de la plupart des exigences de la section 11.2 et les temps de réponse des opérations visant des informations conservées dans des entrepôts éloignés.</i>	
10.10.14	Lorsque le SAE est en mesure de créer des workflows dans les systèmes distribués, il doit pouvoir échanger des données entre ces systèmes afin de contrôler le processus de workflow.	O
10.10.15	Lorsque le SAE gère plusieurs entrepôts et que les « originaux » sont stockés dans des entrepôts particuliers (voir 10.10.4), un administrateur devrait pouvoir modifier l'entrepôt de référence pour les originaux d'une série (avec les séries filles et les documents rattachés) ; si une telle modification se produit, le SAE doit transférer tous les contenus de l'ancien site vers le nouveau.	O
	<i>Ce sera utile en cas de création ou de déplacement d'entrepôt, ou en cas de déplacement de documents vers un autre entrepôt à la suite d'un changement géographique d'activités métier.</i>	
10.10.16	Lorsque le SAE gère plusieurs entrepôts, il devrait permettre à un administrateur d'ajouter un nouvel entrepôt.	O
10.10.17	Lorsque le SAE gère plusieurs entrepôts, il devrait permettre à un administrateur de supprimer un entrepôt.	O

## 10.11 TRAVAIL HORS LIGNE ET A DISTANCE

---

Les exigences de cette section traitent des utilisations à distance et hors ligne du SAE par des utilisateurs qui ne sont pas connectés en permanence au SAE (ou au réseau qui l'héberge).

Plusieurs scénarios sont possibles, notamment :

- les utilisateurs accèdent au SAE via des ordinateurs portables (nomades, bloc-notes...) ou des PC qui sont connectés au SAE de façon intermittente ;
- les utilisateurs se connectent au SAE de l'extérieur par un accès par ligne commutée, ou au travers d'une bande passante faible (par ex : lors d'une session de télétravail ou dans un site provisoire) ;
- les utilisateurs accèdent au SAE par des services mobiles du type PDA ou téléphone intelligent.

Les ordinateurs portables peuvent être utilisés comme des stations de travail normales quand ils sont connectés au SAE. Certains utilisateurs peuvent cependant vouloir télécharger de manière synchrone les documents et données afin d'y travailler hors ligne.

Pour que ce soit possible, le SAE doit télécharger non seulement des lots de documents archivés mais aussi leurs métadonnées. Le SAE devra aussi synchroniser toutes les données modifiées quand l'utilisateur se reconnectera au système.

Parallèlement, les ordinateurs portables peuvent être connectés au SAE de manière intermittente, par exemple avec l'usage du télétravail. Pendant la connexion, l'ordinateur devra se synchroniser avec le SAE. Là aussi, il faudra télécharger les documents, etc., les données téléchargées devant être gérées par l'ordinateur portable entre deux synchronisations.

Les PDA, téléphones intelligents et autres terminaux de poche peuvent être utilisés pour consulter des documents archivés, le plus souvent à l'aide d'une interface de navigation. Les contraintes logistiques telles que la taille de l'écran ou de faibles performances, font que bien souvent ces outils ne pourront offrir toutes les fonctionnalités d'un ordinateur fixe ou portable. Ils sont néanmoins largement utilisés pour la messagerie, les notes ou la tenue des agendas, et il convient alors de synchroniser ces types de documents avec le système central.

MoReq2 ne comporte aucune exigence relative à la maintenance du plan de classement (ex : création d'une nouvelle série) ou des dossiers (ex : clore un dossier) par des utilisateurs nomades ou hors ligne. On pourra développer des systèmes qui le permettent ; MoReq2 ne l'interdit pas.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>10.11.1</b>	Le SAE devrait permettre à un administrateur de préciser les lots d'information qui ne doivent pas être téléchargés.  <i>C'est une mesure préventive de protection de l'information sensible qui, si elle était téléchargée, échapperait au contrôle du SAE.</i>	O
<b>10.11.2</b>	Le SAE doit permettre à un utilisateur de télécharger tout lot de documents avec ses métadonnées pour y travailler quand il n'est pas relié au réseau.	O
<b>10.11.3</b>	Le SAE doit enregistrer dans l'historique des événements toute opération de téléchargement de documents ou de lots de documents.	O
<b>10.11.4</b>	Le SAE devrait ajouter aux métadonnées du document ou du lot le fait que l'entité a été téléchargée pour travail hors ligne.	P
<b>10.11.5</b>	Le SAE doit permettre la synchronisation des documents ou lots téléchargés lors de la connexion au système.  <i>Il s'agit de mettre à jour les métadonnées et d'alerter l'utilisateur si un problème survient.</i>	O

Réf	Exigence	Test
10.11.6	Le SAE doit permettre la mise à jour de l'historique des événements avec les données d'activité hors ligne lors de la connexion au système.	O
10.11.7	Le SAE doit permettre à un utilisateur de capturer des documents créés hors ligne et de les archiver plus tard lorsqu'il se reconnecte au SAE.  <i>Si le document a été créé hors ligne, le SAE doit :</i> <ul style="list-style-type: none"> <li>• lors de la reconnexion, demander à l'utilisateur de le classer directement dans la bonne série, dossier, sous-dossier et volume ;</li> </ul> <i>ou</i> <ul style="list-style-type: none"> <li>• lors de la reconnexion, le déclarer automatiquement sur la base de la série, du dossier, sous-dossier ou volume indiqué préalablement par l'utilisateur (à valider).</li> </ul>	O
10.11.8	Le SAE doit appliquer tous les contrôles d'accès et de sécurité aux outils connectés à distance.  <i>Le SAE ne doit laisser aucune possibilité aux outils portables de briser les règles de sécurité du SAE. Par exemple, un utilisateur ne doit pas pouvoir télécharger une information à laquelle il n'a pas accès en ligne. Ceci dit, MoReq2 reconnaît qu'une information, une fois téléchargée, échappe au contrôle du SAE, et que le SAE ne peut contrer les failles de sécurité après téléchargement.</i>  <i>Les quatre exigences qui suivent ne s'appliquent qu'en cas de GED intégrée au SAE, tel que défini au point 10.3. La même terminologie est utilisée.</i>	P
10.11.9	Le SAE doit permettre à un utilisateur de télécharger des documents avec leurs métadonnées pour y travailler hors connexion au réseau.	O
10.11.10	Le SAE doit donner à un utilisateur la possibilité d'emprunter des documents quand ils sont téléchargés.	O
10.11.11	Si un utilisateur emprunte un document et y travaille hors connexion au SAE, le système doit permettre de lui attribuer un numéro de version.	O
10.11.12	Si un utilisateur emprunte un document et modifie son numéro de version hors connexion, lors de la reconnexion, le SAE doit lui permettre de recharger le document modifié, et doit immédiatement et automatiquement le restituer et enregistrer les modifications et le nouveau numéro de version.	O

## 10.12 INTEGRATION DU FAX

---

*Alors que la messagerie a pris le pas sur le fax comme moyen privilégié de communication rapide pour de nombreuses entreprises/organisations, il existe des cas ou des lieux où le recours au fax reste nécessaire.*

Ce peut être par exemple quand le document original n'existe pas sous forme électronique et qu'il faut en envoyer une copie à une autre entité, où si une reproduction de la signature est demandée.

Certains serveurs de fax sont intégrés aux systèmes de messagerie de sorte que les fax entrants et sortants sont traités comme des pièces jointes de messages. Dans ce cas on appliquera les exigences du point 6.3.

Si le serveur de fax est intégré au SAE, ce sont les exigences suivantes qui s'appliquent.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>10.12.1</b>	Le SAE devrait comporter une interface de programmation (API) pour lui permettre de s'interfacer avec un serveur de fax.	N
<b>10.12.2</b>	Le SAE doit être capable de stocker les fax dans les formats standardisés, par exemple le format image TIFF v6 compression Group IV.  <i>Voir ISO 12033 pour les conséquences des méthodes de compression.</i>	O
<b>10.12.3</b>	Le SAE doit permettre la capture des fax d'une manière intégrée, c'est-à-dire que la capture soit réalisée par un utilisateur à partir de serveur de fax (s'il existe) sans que l'utilisateur ait à se connecter au SAE.	O
<b>10.12.4</b>	Le SAE doit être étroitement intégré pour permettre à un utilisateur de faxer n'importe quel document du SAE qu'il est en train de consulter ou sur lequel il travaille, à partir du SAE (dès lors que le document peut être restitué en deux dimensions).	O
<b>10.12.5</b>	Il doit être possible pour un administrateur de configurer le SAE de telle sorte qu'il effectue une des opérations suivantes lorsqu'un utilisateur du SAE envoie un fax : <ul style="list-style-type: none"> <li>• capturer et archiver automatiquement le document faxé ;</li> <li>• avertir l'utilisateur de la possibilité, s'il le souhaite, d'archiver le document faxé ;</li> <li>• aucune action (l'initiative est laissée à l'utilisateur d'archiver ou non).</li> </ul> <i>Dans l'un ou l'autre cas, on peut admettre que le SAE demande à l'utilisateur de classer manuellement le document et de saisir les métadonnées.</i>	O
<b>10.12.6</b>	Un administrateur doit pouvoir configurer le SAE de telle sorte qu'il effectue une des opérations suivantes quand un utilisateur reçoit un fax : <ul style="list-style-type: none"> <li>• avertir l'utilisateur avec la possibilité, s'il le souhaite, d'archiver le document ;</li> <li>• aucune action (l'initiative est laissée à l'utilisateur d'archiver ou non).</li> </ul> <i>Dans l'un ou l'autre cas, on peut admettre que le SAE demande à l'utilisateur de classer manuellement le document et de saisir les métadonnées.</i>	O

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
10.12.7	<p>Le SAE devrait être capable d'extraire automatiquement les métadonnées des fax entrants, comme l'indique le chapitre 12, soit par exemple :</p> <ul style="list-style-type: none"><li>• titre ;</li><li>• expéditeur ;</li><li>• date et heure ;</li><li>• destinataire.</li></ul> <p><i>Cela peut se faire à l'aide d'un modèle de fax si la structure interne des documents faxés est prédictible.</i></p>	0
10.12.8	<p>Le SAE devrait être capable de renseigner automatiquement les métadonnées des fax sortants, comme l'indique le chapitre 12, soit par exemple :</p> <ul style="list-style-type: none"><li>• titre ;</li><li>• expéditeur ;</li><li>• date et heure ;</li><li>• destinataire.</li></ul> <p><i>Cela peut se faire à l'aide d'un modèle de fax si la structure interne des documents faxés est prédictible.</i></p>	0
10.12.9	<p>Le SAE doit permettre à un utilisateur qui capture un fax de modifier les métadonnées de titre, afin de refléter le contenu réel du fax.</p>	0
10.12.10	<p>Le SAE devrait fournir un type de document « fax » à la fois pour les fax sortants et entrants pour faciliter la saisie de métadonnées par les utilisateurs.</p>	0

## 10.13 NIVEAUX DE SECURITE

---

Le chapitre 4 décrit les exigences pour le contrôle d'accès aux documents, par profil et par groupe. Dans certains environnements (engageant la Défense nationale, la santé...) il est nécessaire de limiter l'accès, à l'aide de niveaux de sécurité et d'habilitations de sécurité.

Ces habilitations priment sur tout droit d'accès reposant sur les critères définis au chapitre 4. Les exigences qui suivent ne s'appliquent qu'aux entreprises/organisations où ce besoin existe.

Il s'agit d'attribuer un ou plusieurs « niveaux de sécurité » aux séries, dossiers, sous-dossiers, volumes et documents. Le terme « niveau de sécurité » est utilisé ici pour désigner « une ou plusieurs données associées à un document archivé pour préciser les règles et conditions d'accès ». L'expression n'est pas très répandue.

Les utilisateurs se voient alors attribuer une habilitation de sécurité qui interdit l'accès à tout groupe de documents dotés de niveaux de sécurité plus élevés.

Les niveaux de sécurité peuvent être divisés en rubriques qui sont soit de nature hiérarchique, soit organisées en fonction d'autres critères spécifiques à une organisation ou à un domaine d'activité.

MoReq2 ne détaille que les exigences pour les rubriques hiérarchiques.

Les exemples ci-après sont basés sur le marquage liée à la Défense nationale mais les principes de marquage dans les autres domaines sont les mêmes.

Il peut exister des exigences de sécurité nationale et de classification propres à tel ou tel pays. Le cas échéant, elles seront traitées dans le chapitre zéro.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>10.13.1</b>	<p>Le SAE doit permettre un des choix suivants au moment de la configuration :</p> <ul style="list-style-type: none"> <li>• niveaux de sécurité attribués aux séries, dossiers, sous-dossiers et/ou volumes (et non à chaque document) ;</li> <li>• niveaux de sécurité attribués à chaque document (et non aux séries, dossiers, sous-dossiers et/ou volumes) ;</li> <li>• niveaux de sécurité attribués à la fois à chaque document et aux séries, dossiers, sous-dossiers et/ou volumes.</li> </ul> <p><i>Certaines entreprises/organisations voudront contrôler l'information sensible au niveau du document, tandis d'autres placeront le contrôle au niveau de la série, du dossier, etc.</i></p>	0
<b>10.13.2</b>	<p>Le SAE doit permettre à un administrateur de préciser, au moment de la configuration, quels profils ont le droit de définir et de modifier les niveaux de sécurité des documents et des entités.</p> <p><i>Dans certaines entreprises/organisations, seuls les propriétaires de l'information ont ce droit. Ailleurs, il peut être partagé entre plusieurs profils s'ils existent (responsables sécurité, cadres).</i></p>	0
<b>10.13.3</b>	<p>Le SAE doit permettre, mais ce n'est pas une obligation, que les niveaux de sécurité soient divisés en rubriques.</p> <p><i>Par exemple, un niveau de sécurité peut être composé de trois rubriques, comme dans l'exemple fictif suivant :</i></p> <ul style="list-style-type: none"> <li>• <i>Niveau ;</i></li> <li>• <i>Avertissement ;</i></li> <li>• <i>Descripteur.</i></li> </ul> <p><i>Chaque rubrique peut être vue comme une des dimensions de la sécurité de l'information. Dans cet exemple, toute combinaison des trois rubriques de sécurité (niveau, avertissement et descripteur) peut s'appliquer au document archivé.</i></p>	0
<b>10.13.4</b>	<p>Le SAE doit exiger la définition et la maintenance de vocabulaires contrôlés par un administrateur, afin de limiter le nombre de valeurs possibles pour chaque rubrique.</p>	0

Réf

Exigence

Test

Par exemple, les rubriques peuvent être celles de l'exemple fictif suivant :

Rubrique	Valeurs possibles
Niveau	Ultra secret Secret Confidentiel Réservé Non classifié
Avertissement	Accès réservé à l'OTAN Accès réservé à l'UEO
Descripteur	Commercial Personnel Direction Audit et contrôle

Dans cet exemple fictif, la rubrique « niveau » est hiérarchique (voir 10.13.6) tandis que les autres ne le sont pas. Les exigences pour les rubriques hiérarchiques sont courantes, voir ci-dessous.

Les exigences pour les rubriques non hiérarchiques peuvent être complexes et sont spécifiques à un domaine d'activité ; à l'exception de l'exigence 10.13.7, elles ne sont pas détaillées ici.

10.13.5

Le SAE devrait permettre la mise en œuvre spécifique de règles de sécurité complexes ou uniques.

N

Cela peut être réalisé par des interfaces de programmation appropriées. Exemples : besoin de gérer des documents qui utilisent des conventions de marquage non prises en compte ici comme celle de l'IDO (International Defence Organisation) ou des restrictions d'accès aux données médicales.

10.13.6

Pour une rubrique au moins, le SAE doit supporter une hiérarchie d'au moins cinq valeurs, depuis l'accès sans restriction jusqu'au plus haut degré de sécurité.

O

La rubrique « Niveau de sécurité » de l'exigence 10.13.3 en est un exemple.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>10.13.7</b>	<p>Lorsqu'une rubrique et les habilitations correspondantes ne sont pas hiérarchiques, le SAE doit permettre de choisir une des options suivantes au moment de la configuration :</p> <ul style="list-style-type: none"> <li>• le SAE doit exiger de tout nouvel utilisateur une habilitation valide ;</li> <li>• le SAE doit appliquer une habilitation par défaut aux nouveaux utilisateurs.</li> </ul> <p>Un administrateur doit pouvoir redéfinir l'habilitation par défaut au moment de la configuration et à tout moment.</p> <p><i>Autrement dit, les habilitations sont obligatoires pour les utilisateurs.</i></p>	0
<b>10.13.8</b>	<p>Si le SAE applique une habilitation par défaut aux nouveaux utilisateurs (cf. 10.13.7), il doit retenir comme habilitation par défaut l'habilitation la plus basse dans la hiérarchie (c'est-à-dire, la plus restrictive).</p>	0
<b>10.13.9</b>	<p>Le SAE doit restreindre l'accès aux documents (séries, dossiers, sous-dossiers et volume, selon la sélection faite au point 10.13.1) aux utilisateurs qui ont un niveau d'habilitation égal ou supérieur au niveau de sécurité.</p> <p><i>A noter que cette habilitation n'est pas toujours suffisante. L'accès aux documents archivés électroniquement peut en outre être limité à certains utilisateurs, profils ou groupes, sur la base des critères définis au chapitre 4.</i></p>	0
<b>10.13.10</b>	<p>Lorsqu'une rubrique est hiérarchique, pour qualifier une nouvelle série, de nouveaux documents, etc., le SAE doit effectuer une des opérations suivantes, à choisir par un administrateur au moment de la configuration (ou plus tard) :</p> <ul style="list-style-type: none"> <li>• le SAE doit appliquer la valeur par défaut choisie par l'administrateur ;</li> <li>• le SAE doit appliquer par défaut la valeur de l'entité mère ;</li> <li>• le SAE doit demander à un administrateur de saisir une valeur.</li> </ul>	0
<b>10.13.11</b>	<p>Lorsqu'une rubrique n'est pas hiérarchique, pour qualifier une nouvelle série, de nouveaux documents, etc., le SAE doit effectuer une des opérations suivantes, à choisir par un administrateur au moment de la configuration (ou plus tard) :</p> <ul style="list-style-type: none"> <li>• le SAE doit appliquer la valeur par défaut choisie par l'administrateur ;</li> <li>• le SAE doit appliquer par défaut la valeur de l'entité mère ;</li> <li>• le SAE doit demander à un administrateur de saisir une valeur.</li> </ul>	0
<b>10.13.12</b>	<p>Quand un nouveau niveau ou une nouvelle rubrique hiérarchique de sécurité est définie, le SAE doit appliquer par défaut à toutes les séries, documents, etc. la valeur la plus basse ; autrement dit, la valeur par défaut doit correspondre au niveau d'accès le plus petit de la hiérarchie.</p>	0
<b>10.13.13</b>	<p>Le SAE devrait permettre l'attribution des habilitations de sécurité à un profil avec possibilité d'héritage. Quand une habilitation est héritée d'un profil, le SAE doit permettre d'appliquer une habilitation différente à l'utilisateur individuel.</p>	0

Réf	Exigence	Test
10.13.14	Si le SAE comporte des niveaux de sécurité à la fois pour les documents et pour les séries, etc. (cf. 10.13.1), il devrait pouvoir interdire qu'une série, un dossier, sous-dossier ou volume ait un niveau de sécurité plus bas que les documents qui y sont classés.	0
10.13.15	Si un utilisateur tente de capturer un document qui a un niveau de sécurité supérieur au groupe dans lequel il est classé, le SAE doit avertir l'utilisateur afin qu'il prenne la mesure appropriée ; le SAE doit permettre au moins une des actions suivantes (paramétrables au moment de la configuration) : <ul style="list-style-type: none"> <li>• le niveau de sécurité de l'entité est aligné sur celui du document ;</li> <li>• l'utilisateur n'est pas autorisé à capturer le document dans cette entité ;</li> <li>• le document est automatiquement transmis à un utilisateur désigné à cet effet pour action ;</li> <li>• l'utilisateur est invité à créer un nouveau groupe pour le document, dotée par défaut des mêmes métadonnées que l'entité de départ ; et à capturer le document dans ce nouveau groupe, dans la suite du processus.</li> </ul>	0
10.13.16	Un administrateur doit pouvoir déterminer le niveau de sécurité le plus élevé d'un document dans n'importe quel(le) série, dossier, sous-dossier ou volume par une simple requête.  <i>Dans certains cas, cette fonction peut grandement faciliter la gestion.</i>	0
10.13.17	En lien avec l'exigence 10.13.1, un administrateur doit pouvoir modifier le niveau de sécurité d'une série, d'un dossier, sous-dossier, volume ou document.  <i>Voir aussi 10.13.27.</i>	0
10.13.18	Le SAE devrait permettre une révision automatique, périodique et programmée des niveaux de sécurité, la révision consistant à : <ul style="list-style-type: none"> <li>• permettre à un utilisateur (dûment habilité et autorisé) de voir certains documents avec leurs niveaux de sécurité ;</li> <li>• permettre à l'utilisateur de modifier les niveaux de sécurité.</li> </ul> <i>MoReq2 ne précise pas les modalités.</i>	0
10.13.19	Le SAE doit systématiquement historiser des valeurs de sécurité dans les métadonnées des documents, séries, etc.	0
10.13.20	Quand un utilisateur modifie la valeur d'un niveau de sécurité (à l'occasion d'une révision comme au point 10.13.18 ou autrement), le SAE doit lui permettre de saisir le motif du changement et doit conserver ce motif comme métadonnée (cf. 10.13.19).  <i>Voir 10.13.2 pour des précisions sur les autorisations de modification des niveaux de sécurité.</i>	0

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>10.13.21</b>	Le SAE doit permettre à l'utilisateur, habilité et autorisé à consulter un document, de voir la valeur du niveau de sécurité et son historique (cf. 10.13.19).	0
<b>10.13.22</b>	Le SAE devrait permettre l'attribution d'un niveau de sécurité à une série, un dossier, sous-dossier ou volume valide pour une période donnée et le dégrader automatiquement au niveau le plus bas à échéance de cette période.	0
<b>10.13.23</b>	Le SAE devrait permettre l'attribution d'un niveau de sécurité à une série, un dossier, sous-dossier ou volume valide pour une période donnée et le dégrader automatiquement pour un niveau inférieur, prédéfini, à échéance de cette période.	0
<b>10.13.24</b>	Le SAE devrait permettre de notifier à l'administrateur l'échéance d'une période d'attribution d'un niveau de sécurité à une série, un dossier, sous-dossier ou volume, et permettre de réévaluer le niveau ou de le corriger.  <i>Par exemple, le SAE enverrait une notification à « date de naissance + X années ». Cela peut servir pour les dossiers médicaux ou pour la protection des données personnelles.</i>	0
<b>10.13.25</b>	Le SAE doit automatiquement enregistrer dans l'historique toutes les modifications aux niveaux et rubriques de sécurité.	0
<b>10.13.26</b>	Le SAE ne doit pas permettre à un utilisateur d'attribuer un niveau de sécurité à une série, un dossier, sous-dossier ou volume auquel il n'a pas accès.	0
<b>10.13.27</b>	Un administrateur doit pouvoir modifier le niveau de sécurité de tous les documents d'une série, d'un dossier, sous-dossier ou volume, et les entités filles (selon de l'option choisie en 10.13.1) en une seule opération.  <i>C'est une mesure courante pour réduire le niveau de protection donné aux documents quand leur confidentialité décroît avec le temps.</i>	0
<b>10.13.28</b>	Le SAE doit permettre d'avertir un administrateur quand le niveau de sécurité de documents est dégradé, et attendre sa confirmation pour achever l'opération.  <i>Cela s'applique particulièrement quand le niveau de sécurité d'un groupe de documents est dégradé à un niveau inférieur à celui des documents qui le composent.</i>	0
<b>10.13.29</b>	Le SAE doit systématiquement historiser toute modification des niveaux de sécurité dans les métadonnées correspondantes de la série, du dossier, sous-dossier, volume ou document.  <i>L'historique doit inclure, pour chaque modification : la date, l'utilisateur, les valeurs ancienne et nouvelle et le motif.</i>	0

# 11. Exigences non fonctionnelles

Le succès d'un système d'archivage électronique ne repose pas que sur ses fonctionnalités. En effet, un certain nombre d'exigences non fonctionnelles y contribue. Elles sont regroupées dans ce chapitre.

Les différentes sections énumèrent les exigences dans les domaines suivants :

- convivialité (section 11.1) ;
- performance et évolutivité (section 11.2) ;
- disponibilité du système (section 11.3) ;
- normes techniques (section 11.4) ;
- environnement législatif et réglementaire (section 11.5) ;
- externalisation et recours à des tiers (section 11.6) ;
- conservation à long terme et obsolescence technologique (section 11.7) ;
- processus métiers (section 11.8).

Ces exigences non fonctionnelles sont souvent difficiles à définir et à mesurer objectivement. Il vaut toutefois la peine de les identifier afin de pouvoir les prendre en considération, au moins à un niveau général. Certaines sont caractéristiques de la GED mais elles sont souvent communes à la plupart des systèmes informatiques.

En outre, les utilisateurs de ces spécifications devront articuler leurs besoins avec les normes techniques et organisationnelles en vigueur. Ils devront également prendre en compte les services d'assistance du fournisseur du SAE : documentation, personnalisation, formation, conseil, etc.

Les entreprises ou administrations devront ajouter leurs propres exigences dans ces domaines, en fonction de leur taille et de leur organisation, des caractéristiques physiques et de l'environnement technique en place. Ce chapitre est conçu comme la liste des points à examiner par les utilisateurs. Ces exigences spécifiques s'ajoutent aux exigences génériques exposées dans les chapitres précédents.

Certains exemples d'exigences utilisent des crochets pour indiquer que l'utilisateur des spécifications doit spécifier une valeur ou une information particulière. Par exemple,

*<xx minutes/heures>*

signifie que l'utilisateur des spécifications devrait saisir une durée, exprimée en minutes ou en heures, pour compléter cette exigence. De même,

*<4 secondes>*

signifie que l'utilisateur des spécifications devrait préciser un intervalle de temps ; les 4 secondes sont proposées à titre d'exemple.

De la même façon, certaines alternatives sont présentées entre crochets. Par exemple :

*<chaque jour/tous les jours ouvrables/xx jours par an>*

signifiera « chaque jour, ou chaque jour ouvrable, ou un nombre de jours par an à définir ou équivalent », selon le souhait de l'entreprise/organisation.

Dans tous les cas de figure, « xx » représente un nombre, petit ou grand.

Du fait de leur caractère générique, et compte tenu que les entreprises/organisations ont des exigences et des priorités très différentes, les exigences non fonctionnelles de ce chapitre ne sont pas intégrées dans le programme de test de MoReq2. Les suggestions de test qui sont données ici le sont à titre indicatif. Les utilisateurs de MoReq2, au vu de leurs exigences spécifiques, fixeront leurs priorités et effectueront leurs propres tests.

## 11.1 CONVIVIALITE

---

Les exigences non fonctionnelles du cahier des charges d'un SAE doivent préciser le degré de convivialité souhaité et sa mise en œuvre. Cela dépendra des types d'utilisateurs ciblés et de l'importance de la formation mise en œuvre. Voir les exemples ci-dessous.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
11.1.1	Le SAE doit permettre à un administrateur de définir à quelle partie du plan de classement chaque utilisateur ou groupe d'utilisateurs peut accéder.  <i>Par exemple, pour un utilisateur ou un groupe d'utilisateurs (les gestionnaires de dossiers sériels, etc.), l'accès peut être limité à une série voire à certains dossiers ou sous-dossiers.</i>	O
11.1.2	Le SAE doit fournir une aide en ligne pour tous les aspects du système.	O
11.1.3	Le SAE doit fournir une représentation graphique du plan de classement hiérarchique et permettre aux utilisateurs d'y naviguer.	O
11.1.4	L'aide en ligne du SAE devrait être contextuelle.	O
11.1.5	Le SAE devrait inclure une aide en ligne pour l'utilisation du plan de classement avec au moins un accès à la description des métadonnées des séries, dossiers, sous-dossiers et volumes.	P
11.1.6	Le SAE devrait inclure un thésaurus pour aider les utilisateurs à choisir les mots clés, les descripteurs, etc.  <i>Voir 11.4.1, 11.4.2 et 11.8.11.</i>	O
11.1.7	Tous les messages d'erreur émis par le SAE doivent être explicites pour que les utilisateurs puissent apporter la correction voulue ou annuler l'opération.  <i>Dans l'idéal, chaque message d'erreur sera accompagné d'un texte explicatif avec la liste des actions propres à résoudre la difficulté.</i>	N
11.1.8	L'interface utilisateurs du SAE devrait être adaptée aux besoins et aux compétences d'utilisateurs très différents ; c'est-à-dire conçue selon les critères d'accessibilité des normes et guides disponibles, et compatible avec les logiciels courants.  <i>Pour les normes et guides, voir l'annexe 7.</i>	N

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>11.1.9</b>	La documentation du SAE doit être fournie dans un format pratique adapté aux besoins et aux compétences d'utilisateurs très différents.  <i>Pour les normes et guides, voir l'annexe 7.</i>	N
<b>11.1.10</b>	Le SAE doit être facile à manipuler, avec une aide intuitive.  <i>La convivialité peut être évaluée par un panel d'utilisateurs représentatifs.</i>	N
<b>11.1.11</b>	Les règles et le fonctionnement de l'interface utilisateurs du SAE doivent être cohérents pour l'ensemble du système : fenêtres, menus et options. Les règles doivent être cohérentes avec le système d'exploitation du SAE.  <i>Les règles devraient être cohérentes avec les principales applications existantes.</i>	P
<b>11.1.12</b>	Le SAE doit être capable d'afficher simultanément plusieurs documents et groupes de documents.	O
<b>11.1.13</b>	Le SAE doit fournir une interface utilisateurs graphique.	O
<b>11.1.14</b>	Le SAE doit permettre aux utilisateurs de déplacer, re-dimensionner et modifier l'apparence des fenêtres, et de sauvegarder ces modifications dans leur profil utilisateur, afin qu'elles soient activées automatiquement à chaque connexion au SAE.	O
<b>11.1.15</b>	Le SAE doit permettre aux utilisateurs de personnaliser l'interface graphique. La personnalisation portera, entre autres, sur les modifications suivantes : <ul style="list-style-type: none"> <li>• le contenu des menus et barres d'outils,</li> <li>• la mise en page des écrans,</li> <li>• l'utilisation des touches de fonction,</li> <li>• les couleurs, polices et tailles des caractères,</li> <li>• les alertes sonores.</li> </ul>	O
<b>11.1.16</b>	Le SAE devrait permettre aux utilisateurs de choisir des alertes sonores (son et volume), et de sauvegarder ces choix dans leur profil utilisateur.	O
<b>11.1.17</b>	Le SAE doit permettre l'affichage systématique de valeurs par défaut selon les besoins. Ces valeurs par défaut seraient notamment : <ul style="list-style-type: none"> <li>• des valeurs définies par l'utilisateur ;</li> <li>• une valeur fixe ;</li> <li>• des valeurs identiques à l'enregistrement précédent ;</li> <li>• des valeurs liées au contexte : date du jour, référence du dossier, identifiant de l'utilisateur ;</li> </ul> selon le cas.	P
<b>11.1.18</b>	Le SAE doit permettre de paramétrer des menus déroulants ou des listes de choix de métadonnées pour la saisie.	O

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
	<i>Le contenu de ces listes devrait être établi par un administrateur.</i>	
<b>11.1.19</b>	Les opérations récurrentes dans le SAE doivent être paramétrées pour être effectuées en un minimum de gestes (clics de souris ou commandes clavier).	P
<b>11.1.20</b>	Le SAE devrait être étroitement intégré au système de messagerie de l'entreprise/organisation afin qu'un utilisateur puisse envoyer électroniquement des documents ou des groupes de documents sans quitter le SAE.  Par exemple, un utilisateur doit pouvoir envoyer un courrier client à partir du SAE. <i>L'objectif</i> est que l'utilisateur n'ait pas à se déconnecter pour transmettre un document archivé.	N
<b>11.1.21</b>	Si le point 11.1.20 est acquis, le SAE devrait envoyer des pointeurs ou des liens vers les groupes de documents ou les documents plutôt que des copies, si toutefois l'envoi est destiné à un autre utilisateur du SAE.  <i>Il peut y avoir des exceptions, par exemple pour un utilisateur éloigné qui n'a pas accès à la base centrale.</i>	N
<b>11.1.22</b>	Le SAE devrait indiquer si le message électronique a une pièce jointe.  <i>Par exemple au moyen d'une icône.</i>	O
<b>11.1.23</b>	Le SAE devrait autoriser des fonctions programmables par l'utilisateur.  <i>Par exemple des macros créées par les utilisateurs.</i>	O
<b>11.1.24</b>	Lorsque les utilisateurs doivent saisir des métadonnées pour des documents numérisés (images de documents papier), le SAE devrait permettre le recours à la reconnaissance optique de caractères pour capturer les métadonnées à partir de l'image (OCR sur zone).  <i>L'utilisateur doit pouvoir par exemple sélectionner la zone de l'image qui contient les métadonnées de date ou de titre, puis océriser cette image et déclarer le résultat comme métadonnées, tout cela en une seule opération.</i>	O
<b>11.1.25</b>	Le SAE devrait permettre aux utilisateurs de définir des références croisées entre les documents, au sein du même groupe ou à travers différents groupes, pour faciliter la navigation entre les documents.	O
<b>11.1.26</b>	Quand il consulte ou travaille sur un document ou un groupe de documents (série, dossier, sous-dossier ou volume), qu'il s'agisse ou non d'un résultat de recherche, l'utilisateur devrait pouvoir utiliser les fonctions du SAE pour trouver facilement une information dans le groupe immédiatement supérieur sans quitter ou fermer le document.  <i>L'utilisateur doit pouvoir par exemple repérer dans quelle série, dans quel dossier, sous-dossier ou volume se situe le document consulté ; s'il voit les métadonnées du dossier, il doit voir la série de rattachement.</i>	O
<b>11.1.27</b>	Le SAE devrait permettre à l'utilisateur qui accède à un dossier ou à un document de vérifier si un autre utilisateur, groupe ou profil y a accès.	O

Réf	Exigence	Test
	<i>Ceci doit permettre de signaler explicitement un utilisateur, un groupe ou un profil. Ainsi, un utilisateur peut s'enquérir des droits d'un autre sur tel ou tel document ou dossier, sans connaître forcément les membres du groupe ou du profil.</i>	
11.1.28	<p>Le SAE devrait permettre à un utilisateur de réduire le risque d'erreur de classement par un verrou temporaire posé en un clic sur un dossier ou un document. Ce verrou devrait interdire l'accès du document ou du dossier aux autres utilisateurs (excepté l'administrateur); le SAE devrait informer systématiquement l'administrateur qu'un verrou temporaire a été posé, lui seul et nul ayant la faculté de le retirer.</p> <p><i>Ceci doit permettre aux utilisateurs de corriger une erreur - document confidentiel classé par inadvertance (par glisser/lâcher) dans un dossier non sécurisé par exemple. Les utilisateurs n'ayant pas le droit de supprimer, retirer ou modifier les documents archivés, il faut l'intervention d'un administrateur.</i></p> <p><i>Pour éviter l'abus de cette facilité, il est important que les utilisateurs soient formés à l'utilisation du verrou temporaire et que les administrateurs vérifient qu'ils n'en abusent pas.</i></p>	O
11.1.29	<p>Les utilisateurs devraient pouvoir faire des copies des documents du SAE sur leur poste de travail, dans d'autres environnements, par un simple glisser/lâcher sans que le document ou ses métadonnées en soient affectés.</p> <p><i>Quand la copie d'un document est transposée dans un autre environnement, on peut accepter de perdre ses métadonnées (du fait même que la plupart des applications ne reconnaissent pas le modèle de métadonnées de MoReq2).</i></p>	P
11.1.30	<p>Le SAE devrait fournir une aide en ligne qui soit visuelle.</p> <p><i>Par exemple, avec des copies d'écran et/ou des animations montrant aux utilisateurs comment procéder.</i></p>	P
11.1.31	<p>Le SAE devrait permettre aux utilisateurs de marquer certaines fonctions d'aide comme « favoris » ou équivalent afin de les retrouver plus facilement une autre fois.</p>	O
11.1.32	<p>Un utilisateur qui travaille sur un dossier doit pouvoir trouver facilement et rapidement les mots-clés de ce dossier.</p> <p><i>Il faut pouvoir retrouver les mots-clés sans avoir à quitter le dossier, de sorte que le travail sur le dossier ne soit pas interrompu.</i></p>	O
11.1.33	<p>Le SAE devrait permettre aux utilisateurs de marquer comme favoris des séries, des dossiers ou des documents, afin de les retrouver plus facilement une autre fois.</p>	O
11.1.34	<p>Le SAE devrait permettre aux utilisateurs de transmettre leurs favoris à d'autres utilisateurs.</p>	O

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
	<i>Les favoris peuvent être envoyés par messagerie ou par une autre voie.</i>	

## 11.2 PERFORMANCE ET EXTENSIBILITE

---

Il serait utile d'évaluer dans quelle mesure le SAE fournit des temps de réponse conformes aux attentes des utilisateurs et s'il peut s'adapter aux différentes tailles de populations auquel il est destiné. Voir les remarques et les exemples d'exigences ci-dessous.

Les temps de réponse aux utilisateurs dépendront aussi de facteurs extérieurs au SAE, par exemple :

- bande passante du réseau ;
- utilisation du réseau ;
- latence du réseau ;
- configuration et utilisation des ressources des différents serveurs.

Ces spécifications ne peuvent pas traiter des facteurs externes sinon pour rappeler qu'ils ne peuvent être ignorés. Normalement, des tests grandeur nature sont nécessaires pour avoir une vision fiable de la performance.

En conséquence, les exigences ci-dessous devraient être interprétées par rapport à des temps de réponse standard. Ces standards peuvent varier d'un environnement à l'autre, selon le type d'infrastructure.

Par exemple, si le SAE est défini pour une infrastructure existante, il peut être opportun de définir les temps de réponse comme le laps de temps entre la réception d'une requête par le serveur et l'envoi de la réponse ; inversement, si le SAE est conçu pour un nouveau réseau, il peut être préférable de définir les temps de réponse comme le laps de temps entre la saisie de la requête et l'affichage de la réponse sur le poste de travail.

Les exigences spécifiques pour le travail hors ligne ou à distance figurent dans la section 10.11 et devront du reste être adaptées à l'environnement.

Le SAE doit être capable d'effectuer toutes les fonctions de manière cohérente pour les besoins métier et utilisateurs selon les modèles d'exigences ci-dessous.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
------------	-----------------	-------------

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>11.2.1</b>	<p>Le SAE doit fournir des temps de réponse adaptés aux besoins métier pour les fonctions courantes exécutées dans des conditions normales, par exemple :</p> <ul style="list-style-type: none"> <li>• &lt;100%&gt; de la population estimée pour le système, connectée et active ;</li> <li>• &lt;100%&gt; du volume total estimé de documents effectivement gérés par le système ;</li> <li>• des utilisateurs effectuant différents types de transaction à des débits variés ;</li> <li>• avec une performance d'au moins dix transactions.</li> </ul>	N
<b>11.2.2</b>	<p>Le SAE doit pouvoir restituer les résultats dans les &lt;3 secondes&gt; pour une simple recherche et &lt;10 secondes&gt; pour une recherche complexe (combinant quatre termes), quels que soient la capacité de stockage ou le nombre des dossiers et documents gérés.</p> <p><i>Dans ce contexte, l'exécution d'une recherche signifie produire une liste de résultats (voir 8.1.10) et n'inclut pas l'accès aux documents eux-mêmes.</i></p>	N
<b>11.2.3</b>	<p>Le SAE doit pouvoir retrouver et afficher dans les &lt;4 secondes&gt; la première page d'un document consulté au cours des &lt;xx&gt; mois précédents, quels que soient la capacité de stockage ou le nombre des dossiers et documents gérés.</p> <p><i>Cette exigence, comme celle du point 11.1.4, ne s'applique qu'aux documents en format page. Pour des documents de dimensions exceptionnelles, le temps de réponse acceptable sera allongé.</i></p> <p><i>L'expression « au cours des &lt;xx&gt; mois précédents » suppose la présence d'un mécanisme de stockage étagé ou hiérarchique. Voir aussi l'exigence suivante.</i></p> <p><i>Cette exigence vise à permettre une recherche rapide des documents les plus utilisés, en supposant que fréquence d'utilisation rime avec utilisation récente. L'entreprise/organisation précisera les délais à partir desquels la fréquence de consultation décroît.</i></p>	N
<b>11.2.4</b>	<p>Le SAE doit pouvoir retrouver et afficher dans les &lt;20 secondes&gt; la première page d'un document qui n'a pas été consulté au cours des &lt;xx&gt; mois précédents, quels que soient la capacité de stockage ou le nombre des dossiers et documents gérés.</p> <p><i>Cette exigence concerne les cas d'utilisation d'une forme de stockage hiérarchique, où les documents plus rarement consultés sont stockés sur des supports de performance moindre que les documents actifs, ou en proximité. L'entreprise/organisation précisera les délais à partir desquels la fréquence de consultation décroît.</i></p> <p><i>Ceci dit, si tous les documents électroniques archivés sont stockés dans un système simple (i.e. sans stockage étagé ou hiérarchique), l'expression « au cours des &lt;xx&gt; mois précédents », inappropriée, devra être supprimée.</i></p>	N

Réf	Exigence	Test
11.2.5	<p>Le SAE doit permettre une implémentation unique du système avec une capacité de stockage électronique d'au moins &lt;xx gigaoctets/teraoctets/pétooctets&gt; ou &lt;xx milliers/millions/milliards&gt; de documents, desservant au moins &lt;xx centaines/milliers&gt; d'utilisateurs simultanés avec la performance requise dans cette section.</p> <p><i>L'entreprise/organisation précisera ses besoins de stockage et les fourchettes de documents et d'utilisateurs. Dans de grandes entreprises les volumes peuvent être très importants et atteindre les milliards d'informations archivées.</i></p>	N
11.2.6	<p>Le SAE doit fournir des niveaux de performance indiqués dans cette section au minimum pour les volumes suivants :</p> <ul style="list-style-type: none"> <li>• &lt;xx&gt; séries ;</li> <li>• &lt;xx&gt; dossiers par série ;</li> <li>• &lt;xx&gt; sous-dossiers par dossier ;</li> <li>• &lt;xx&gt; volumes par sous-dossier ;</li> <li>• &lt;xx&gt; documents par volume.</li> </ul> <p><i>Ces éléments sont purement indicatifs. L'entreprise/organisation avisera si d'autres indicateurs répondent à ses besoins.</i></p>	N
11.2.7	<p>Il doit être possible d'étendre le SAE, d'une manière contrôlée, pour répondre à une croissance de la population d'au moins &lt;xx centaines/milliers&gt; d'utilisateurs, sans rupture de continuité du service.</p> <p><i>Le but de cette exigence est que l'extension puisse se faire progressivement sans interruption majeure de la disponibilité du système.</i></p>	N
11.2.8	<p>Le SAE doit permettre ces niveaux de performance avec une maintenance :</p> <ul style="list-style-type: none"> <li>• des profils, utilisateurs et groupes d'utilisateurs ;</li> <li>• des niveaux de sécurité ;</li> <li>• des droits d'accès ;</li> <li>• des plans de classement ;</li> <li>• des bases de données ;</li> <li>• des règles de conservation/destruction ;</li> <li>• des gels de destruction ;</li> </ul> <p>en vue de changements organisationnels prévisibles, sans imposer des indisponibilités du système ou un surcroît d'administration (voir aussi le chapitre 9).</p> <p><i>Si les exigences de performance sont strictes, il peut être nécessaire de quantifier les changements organisationnels.</i></p>	N
11.2.9	<p>Le SAE doit être extensible et doit pouvoir être utilisé dans de petites ou grandes entreprises/organisations, avec des entités de tailles hétérogènes et en nombre variable et des localisations géographiques différentes.</p>	N

## 11.3 DISPONIBILITE DU SYSTEME

---

Dans de nombreux cas, l'introduction conjointe d'un SAE et d'une GED augmentera la dépendance des utilisateurs envers le réseau informatique au point qu'ils pourront se trouver dans l'incapacité de continuer leur travail si le SAE / la GED ne fonctionnent pas.

En conséquence, les utilisateurs de ces spécifications à la recherche d'un système devraient s'efforcer d'identifier les exigences de disponibilité et les indiquer dans le cahier des charges. Voir les exemples ci-dessous.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>11.3.1</b>	Le SAE doit être accessible aux utilisateurs : de <xx :00> à <xx :00> <chaque jour/tous les jours ouvrables/xx jours par an>.	N
<b>11.3.2</b>	Les indisponibilités planifiées du SAE ne doivent pas excéder <xx> heures par <trimestre glissant>.	N
	<i>La définition des indisponibilités peut dépendre de l'infrastructure et de l'architecture. Par exemple, dans certains environnements, une panne causée par un serveur sera considérée comme une panne du SAE ; dans d'autres cas, cette panne sera analysée différemment et ne sera pas imputable au SAE.</i>	
	<i>Il convient de s'accorder sur une définition ; comme base de travail, on peut proposer : « Le SAE est dit indisponible si plus de &lt;xx%&gt; des utilisateurs sont dans l'incapacité d'exécuter les fonctions courantes du SAE et si cette panne est imputable à une composante du SAE autre que le poste de travail.</i>	
<b>11.3.3</b>	Les indisponibilités non planifiées du SAE ne doivent pas excéder <xx> heures par <trimestre glissant>.	N
	<i>Dans un cahier des charges, il peut être pertinent de demander des garanties quant au temps moyen de résolution des problèmes de ce type.</i>	
<b>11.3.4</b>	Le nombre d'incidents dus aux indisponibilités non planifiées du SAE ne doit pas excéder <xx> heures par <trimestre glissant>.	N
	<i>Dans un cahier des charges, il peut être pertinent de demander des garanties quant au temps moyen entre deux pannes de ce type.</i>	
<b>11.3.5</b>	En cas de panne logicielle ou matérielle, il doit être possible de restaurer un état précédent du SAE (pas avant <la sauvegarde de la veille>) dans les <xx> heures suivant la restauration du matériel.	N

## 11.4 NORMES TECHNIQUES

---

Le SAE devrait être conforme aux normes de droit et de fait du domaine. Dans la mesure du possible, le SAE devrait utiliser des interfaces ouvertes plutôt que propriétaires.

Les utilisateurs de ces spécifications auront à préciser leurs exigences dans les domaines suivants :

- environnement matériel (plates-formes, postes de travail) ;
- environnement du système d'exploitation (plates-formes, postes de travail) ;
- architecture logicielle des postes de travail (client) ;
- interface utilisateurs ;
- base de données relationnelle et interface ;
- protocole réseau et système d'exploitation ;
- normes d'échange ;
- l'interface de programmation et les kits de développement.

Lors de l'utilisation de ces spécifications pour un cahier des charges, il sera nécessaire de préciser l'environnement technique, notamment toutes les interfaces du SAE (système patrimonial, système administratif) ainsi que les prévisions d'évolution.

En outre, les utilisateurs de ces spécifications prendront en compte leurs exigences particulières en matière de normalisation.

*Voir l'annexe 7 pour la liste complète des normes citées dans ces spécifications.*

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>11.4.1</b>	Si le SAE est doté d'un thésaurus monolingue, il devra être conforme à la norme ISO 2788 - Principes directeurs pour l'établissement et le développement de thésaurus monolingues.	O
<b>11.4.2</b>	Si le SAE est doté d'un thésaurus multilingue, il devra être conforme à la norme ISO 5964 - Principes directeurs pour l'établissement et le développement de thésaurus multilingues.	O
<b>11.4.3</b>	Le SAE doit permettre le stockage de documents dont les formats de fichiers et d'encodage sont soit normalisés, soit complètement documentés.  <i>Les entreprises/organisations utilisatrices peuvent désirer des formats de fichiers et d'encodage spécifiques.</i>	P
<b>11.4.4</b>	Le SAE devrait stocker toutes les dates dans un format conforme à ISO 8601 - Éléments de données et formats d'échange - Échange d'information - Représentation de la date et de l'heure.	O
<b>11.4.5</b>	Le SAE devrait comporter tous les noms de langue dans un format conforme à ISO 639 - Codes pour la représentation des noms de langue.	O
<b>11.4.6</b>	Si le SAE doit gérer des documents en plusieurs langues ou utilisant des caractères non latins, il devrait pouvoir utiliser l'encodage ISO 10646 (Unicode).	O

## 11.5 ENVIRONNEMENT LEGISLATIF ET REGLEMENTAIRE

---

Le SAE doit se conformer à l'environnement législatif et réglementaire qui varie forcément d'un pays à l'autre et selon les domaines d'activité.

MoReq2 ne traite pas des obligations de conservation des archives physiques. Cette obligation peut exister ou non, selon l'environnement législatif et réglementaire ; si c'est le cas, on doit veiller à préserver l'intégrité et l'exploitabilité des archives électroniques et physiques comme un tout. Ces questions feront l'objet de politiques organisationnelles spécifiques.

Les exigences qui suivent seront regroupées dans le chapitre zéro.

En outre, les utilisateurs de MoReq2 prendront en compte leurs exigences particulières à leur domaine d'activité, au marché, etc.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
11.5.1	Le SAE doit respecter les normes nationales concernant l'admissibilité en preuve et la force probante des documents électroniques.	N
11.5.2	Le SAE doit se conformer à la législation nationale sur l'archivage et le records management.	N
11.5.3	Le SAE ne doit comporter aucun élément qui soit incompatible avec la législation nationale en termes de protection des données, liberté de l'information ou autre.	N
11.5.4	Le SAE doit se conformer aux exigences réglementaires européennes, nationales ou locales, aux directives ou aux codes de bonnes pratiques du secteur d'activité concerné.	N

## 11.6 EXTERNALISATION DES DONNEES ET RECOURS A DES TIERS

---

De nombreuses entreprises/organisations utilisent des prestataires pour stocker et gérer des documents archivés. Il s'agit parfois de documents qui ne sont plus actifs (ou qui sont très peu consultés) mais qui doivent être conservés en application d'une durée légale ou administrative de conservation, ou de règles industrielles, ou qui sont destinés à une conservation à long terme.

D'autres organisations ont recours à des fournisseurs de services applicatifs (ASP) pour gérer les documents archivés qui sont actifs aussi bien que ceux qui ne le sont plus. Ces documents - factures, correspondance clients, demandes de prêt hypothécaire, etc. - sont envoyés au prestataire pour indexation et stockage. Ils sont alors repérables et consultables par les collaborateurs de l'entreprise/organisation via Internet ou un Extranet.

La gestion des documents archivés électroniquement par un tiers exigent que le contrat avec le prestataire de service énonce clairement les procédures et les contrôles pour la conformité aux exigences réglementaires, le respect des bonnes pratiques pour l'admissibilité en preuve des documents électroniques, et la satisfaction des besoins métier en termes d'accès et de disponibilité.

Le contrat doit comporter des clauses précisant que :

- la qualité de la gestion chez le prestataire de service doit être au moins égal à celle du client pour son archivage interne ;
- le client pourra récupérer ultérieurement les documents auprès du prestataire de telle sorte qu'il puisse poursuivre la gestion des documents archivés conformément aux normes en vigueur et satisfaire aux exigences d'admissibilité en preuve.

*Cette sous-section s'appuie largement sur la norme ISO 15801 (voir annexe 7).*

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>11.6.1</b>	Un contrat ou engagement de service, détaillant les prestations, doit être conclu avec le prestataire.  <i>Un engagement de service est un contrat négocié entre le client et le prestataire. Il consigne l'accord entre les parties sur les prestations, les priorités, les responsabilités, etc.</i>	N
<b>11.6.2</b>	Les procédures de transfert des documents archivés du client vers le prestataire et du prestataire vers le client doivent être décrites en détail.  <i>Il peut s'agir de liens de communication entre les sites avec transfert automatique des dossiers et des documents, quotidiennement ou régulièrement. Le client doit être assuré que le lien entre les deux sites est sécurisé, qu'il existe un protocole de contrôle des documents reçus et de suivi des anomalies.</i>	N
<b>11.6.3</b>	Le prestataire doit pouvoir fournir au client une copie de l'historique traçant le processus d'entrée et de stockage des documents/dossiers.	N
<b>11.6.4</b>	Le prestataire doit prouver que les dossiers/documents et leurs métadonnées hébergés peuvent être renvoyés facilement vers le SAE du client sans aucune perte de structure, de métadonnées ou de contenu des documents.	N
<b>11.6.5</b>	Le prestataire doit avoir des procédures qui permettent au client de transférer des dossiers et des documents individuellement.	N
<b>11.6.6</b>	Le prestataire doit pouvoir fournir au client un accès direct aux documents hébergés. Il doit lui délivrer soit une reproduction du document archivé, soit le document original, dans les temps et au tarif convenus.	N
<b>11.6.7</b>	Le prestataire devrait pouvoir permettre au client d'effectuer des requêtes, de visualiser et d'imprimer les documents et/ou dossiers depuis ses bureaux.  Ceci peut se faire, par exemple, via une connexion réseau.	N
<b>11.6.8</b>	Le prestataire devrait pouvoir permettre au client de demander en ligne le téléchargement ou la transmission de documents et/ou de dossiers entre le SAE du client et les solutions de stockage du prestataire.	N

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
11.6.9	Le client devrait pouvoir demander des statistiques sur les documents hébergés, sur les échéances de durées de conservation, etc. Ceci devrait pouvoir se faire en ligne, depuis les bureaux du client.	N
11.6.10	Les prestations énoncées en 11.6.7, 11.6.8 et 11.6.9 devraient : <ul style="list-style-type: none"><li>• avoir des délais de réponse et de livraison contractualisés ;</li><li>• être effectuées dans un environnement sécurisé.</li></ul>	N
11.6.11	Le client devrait vérifier que les locaux du prestataire sont corrects et obéissent aux critères de sécurité correspondant à ses besoins.	N
11.6.12	Le client devrait vérifier que les procédures proposées et la gestion du stockage ne présentent pas plus de risques pour les documents que ses propres procédures.  <i>Le prestataire devra prouver que tous les documents du client sont sauvegardés et que, en cas de panne du système, ils peuvent être récupérés dans les délais contractualisés.</i>	N
11.6.13	Le client devrait vérifier que le prestataire emploie un personnel fiable lorsque les documents sont particulièrement sensibles.  <i>La signature d'un engagement de confidentialité par tous les employés du prestataire au moment de leur recrutement est un plus.</i>	N
11.6.14	Tout envoi de documents entre le client et le prestataire devrait être accompagné d'un bordereau comportant l'identification et le nombre des documents et dossiers transmis.	N
11.6.15	Les tiers prestataires de transport devraient répondre aux exigences de qualité et de fiabilité du client.	N

## 11.7 CONSERVATION A LONG TERME ET OBSOLESCENCE TECHNOLOGIQUE

---

### Contexte

La conservation à long terme des documents archivés électroniquement est confrontée à trois types de risques technologiques :

- dégradation des supports ;
- obsolescence du matériel ;
- obsolescence des formats.

Ces risques sont analysés sommairement ci-dessous. Pour plus de détails, on se reportera à ISO 18492 et à diverses publications diffusées par les institutions archivistiques et patrimoniales.

## Dégradation des supports

Le risque de dégradation des supports tient au fait que tous les supports de stockage numériques ont une durée de vie limitée. La durabilité varie d'un support à l'autre et avec les conditions environnementales.

Les précautions suivantes peuvent éviter des pertes d'information dues à la dégradation des supports :

- s'assurer que tous les supports sont stockés, utilisés et manipulés dans des conditions environnementales satisfaisantes ;
- remplacer régulièrement les supports (en recopiant l'information sur de nouveaux supports) avant la fin de vie théorique ;
- conserver plusieurs copies de chaque document et comparer systématiquement et régulièrement les copies. Cette démarche est notamment celle des centres d'archivage de données spécialisés dans le long terme ; elle exige des systèmes automatisés dont la description détaillée dépasse le cadre de ces spécifications.

## Obsolescence du matériel

Les périphériques de stockage - lecteurs de bandes et de disques - ont une durée de vie limitée. Quand ils atteignent ou dépassent cette durée de vie, ils exigent forcément plus de maintenance, alors même que la maintenance et la réparation deviennent plus coûteuses ; au bout du compte, il devient quasiment impossible de les réparer. L'information stockée sur des supports obsolètes sera définitivement perdue si le dispositif tombe en panne, à moins qu'elle n'ait été recopiée sur d'autres supports.

## Obsolescence des formats

L'obsolescence des formats constitue la principale difficulté dès que l'on dépasse quelques années.

Le problème tient au fait que la plupart des protocoles et composants logiciels intervenant dans la chaîne de traitement entre le support et la restitution des données sont en constante évolution. Ce sont : les normes d'encodage, les formats de fichiers, et les logiciels. L'évolution est rapide et n'offre pas toujours de compatibilité - c'est particulièrement vrai au-delà de quelques années. Les techniques suivantes sont généralement reconnues :

- migration (conversion de l'information vers de nouveaux formats accessibles par les matériels et logiciels courants) ;
- émulation (transfert de l'information vers un nouveau matériel avec ajout d'un composant logiciel qui émule l'ancien matériel, permettant ainsi l'exécution de l'ancienne application) ;
- conservation technologique (maintenance permanente du matériel d'origine ; mais c'est irréaliste sur le long terme) ;
- encapsulation des données et du logiciel (approche théorique qui suppose un regroupement des documents, des métadonnées, du SAE et des autres applicatifs dans un logiciel « enveloppe »).

Il n'existe pas à ce jour de méthode simple et générique qui garantisse l'accès aux documents électroniques sur le long terme. On s'accorde à dire que :

- la stratégie la plus pertinente est de ne stocker l'information que dans des formats largement répandus, stables et ouverts (c'est-à-dire complètement documentés et dont les spécifications sont publiées) et dont la durée de vie est réputée longue, tel XML et PDF/A ;

- la migration et/ou l'émulation sont considérées comme les solutions les plus sûres ; en pratique, les deux exigent la préservation de métadonnées - voir plus loin.

Les exigences ci-après prennent en compte les différentes approches. Pour plus d'information, voir l'annexe 7.

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>11.7.1</b>	Les supports de stockage du SAE doivent être utilisés et stockés dans des environnements compatibles avec la durée de vie souhaitée ou prévue, en général inférieure aux prévisions des fabricants.	N
<b>11.7.2</b>	Le SAE doit permettre le contrôle et le remplacement des supports de stockage afin de prévenir la dégradation des supports.  <i>Ceci suppose que le SAE, ou le sous-système de stockage qu'il utilise, gère les taux d'erreur des supports et permet le remplacement des supports fautifs ou en fin de vie, sans endommager les documents.</i>	O
<b>11.7.3</b>	Le SAE devrait inclure des fonctionnalités de comparaison automatique et périodique des copies réalisées et le remplacement de toute copie fautive, afin de prévenir la dégradation des supports.	P
<b>11.7.4</b>	Le SAE doit permettre une migration (conversion) en masse des documents (avec leurs métadonnées et l'historique des événements) vers de nouveaux supports et/ou systèmes suivant les normes régissant leur(s) format(s).	O
<b>11.7.5</b>	Le fournisseur du SAE doit posséder un programme de mise à jour du système qui garantit la continuité de l'accès à l'information existante sans modification des contenus.	N
<b>11.7.6</b>	Toute modification opérée sur le SAE pour des raisons organisationnelles doit être maintenue en cas de mise à jour du système.	N
<b>11.7.7</b>	Le SAE devrait pouvoir fournir des statistiques sur les formats de fichiers, les versions et les composants.  <i>Par exemple, le SAE devrait pouvoir produire des listes de composants de formats prédéfinis. Cette fonction serait couplée à un logiciel intelligent ou une fonction de pilotage de la conservation visant à identifier les formats de fichiers susceptibles d'obsolescence.</i>	O
<b>11.7.8</b>	Le SAE devrait pouvoir restituer (voir le glossaire) les documents archivés à partir de leur format d'origine dans un format de conservation à long terme prédéfini, lors de la capture, plus tard, ou lors d'un export.  <i>On peut admettre que le processus de restitution soit initié par un programme extérieur au SAE dès lors que le contexte et les liens sont préservés durablement.</i>	P
<b>11.7.9</b>	Quand cela est possible sans porter atteinte à l'intégrité des documents, le SAE devrait pouvoir convertir les composants à partir de leur format d'origine dans un format de conservation à long terme prédéfini, au moment de la capture, plus tard, ou lors d'un export.	P

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
	<p><i>On peut admettre que le processus de restitution soit exécuté par un programme extérieur au SAE dès lors que le contexte et les liens sont préservés durablement.</i></p> <p><i>Il est essentiel que l'intégrité des documents constitués de composants restitués soit maintenue. La faisabilité de cette approche dépend en général à la fois de la qualité du processus de conversion et du logiciel ou du visualiseur utilisé. Par exemple, s'il s'agit de pages web comportant des images GIF, on peut admettre la conversion des seules images GIF si les conditions suivantes sont toutes remplies :</i></p> <ul style="list-style-type: none"> <li><i>• les composants GIF sont convertis dans un format exécutable par l'application utilisée pour accéder aux pages web ; dans cet exemple, ce pourrait être JPEG ;</i></li> <li><i>• les références aux images GIF des pages web sont modifiées au cours du processus de migration afin de renvoyer aux nouvelles images JPEG ;</i></li> <li><i>• les composants originaux (les pages web initiales et les composants GIF initiaux) sont conservés à côté des nouveaux composants.</i></li> </ul> <p><i>Le SAE doit au minimum permettre ces opérations et devrait au mieux les effectuer automatiquement.</i></p> <p><i>Cet exemple est donné à titre d'illustration ; il ne sous-entend à ce jour aucune recommandation de migrer les images GIF.</i></p>	
<b>11.7.10</b>	En cas de restitution de documents ou de composants, le SAE doit permettre à l'administrateur qui effectue la conversion d'en saisir le motif.	O
<b>11.7.11</b>	<p>Quand un document a fait l'objet d'une restitution dans un format de conservation, le SAE doit faciliter la recherche du format original et/ou des conversions, selon le cas.</p> <p><i>Voir aussi 5.2.3.</i></p>	P
<b>11.7.12</b>	Le SAE devrait pouvoir exporter des documents et leurs métadonnées sous la forme d'un Paquet d'information diffusé (DIP) tel que le définit le modèle OAIS, ISO 14721, annexe 7.	O
<b>11.7.13</b>	<p>Le SAE devrait conserver au minimum les métadonnées suivantes dans la conversion d'un composant :</p> <ul style="list-style-type: none"> <li>• le format original et sa version ;</li> <li>• la date de conversion.</li> </ul>	O
<b>11.7.14</b>	<p>Le SAE devrait pouvoir extraire les métadonnées techniques incluses dans un composant et les stocker comme métadonnées.</p> <p><i>Ces métadonnées s'ajouteront aux métadonnées indiquées dans le modèle de métadonnées de MoReq2. Ce peut être par exemple les détails techniques d'une image tels que les métadonnées du format TIFF v6, ou l'ordre des octets (petit ou grand indien), la longueur ou la largeur de l'image.</i></p>	P

Réf	Exigence	Test
11.7.15	<p>Si le SAE utilise des structures d'encodage, de stockage ou de base de données propriétaires, elles doivent être complètement documentées, et la documentation accessible aux administrateurs.</p> <p><i>Le fait que le fournisseur garde une copie de sa documentation risque de ne pas être suffisant ; pour la période à considérer, la pérennité du fournisseur n'est pas garantie. On peut dès lors souhaiter qu'une copie de la documentation soit remise à l'entreprise/organisation utilisatrice ou à un tiers.</i></p>	O
11.7.16	<p>Le SAE devrait pouvoir gérer une série de métadonnées de conservation pour les documents et leurs composants.</p> <p><i>Voir annexe 9.</i></p>	P
11.7.17	<p>Le code source du SAE devrait soit être ouvert soit faire l'objet d'un contrat de dépôt chez un tiers de confiance.</p>	N

## 11.8 PROCESSUS METIER

---

L'expérience montre que le succès de la mise en œuvre d'un SAE dépend, entre autres facteurs, de sa compatibilité avec les pratiques des équipes sur le terrain. Même si un SAE comporte toutes les fonctions requises pour l'archivage, la GED, etc. sa mise en œuvre ne sera réussie que si les utilisateurs considèrent qu'il est facile à utiliser. Dans le cas contraire, il sera rejeté en dépit de ses qualités.

Partant de ce constat, cette section énonce les exigences visant à la flexibilité et à la facilité d'utilisation. C'est pourquoi, la plupart des exigences qui suivent sont souhaitables et non obligatoires. Elles peuvent être satisfaites par le biais d'un workflow intégré dans le SAE.

Certaines des exigences qui suivent plaident pour une fonction définie « comme partie intégrante du processus ». Dans tous les cas, cela sous-entend qu'un utilisateur effectuant une opération devrait :

- pouvoir choisir entre exécuter ou non le processus ;
- pouvoir initier l'opération facilement, si possible d'un simple clic, sans avoir besoin de ressaisir une information préalablement saisie ;
- pouvoir décider à la fin de l'opération d'annuler le processus ou de revenir à son point de départ et retrouver son statut d'avant le lancement de l'opération (sans avoir besoin de ressaisir une information préalablement saisie).

*Voir l'illustration en figure 11.1.*

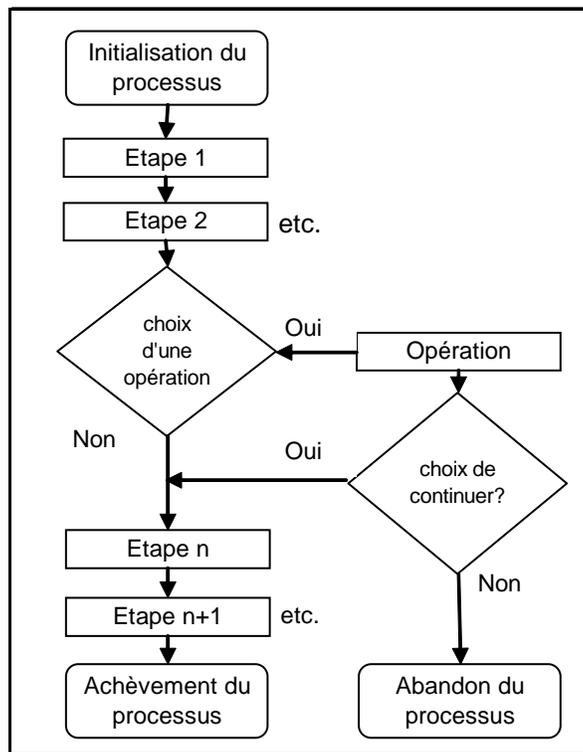


Figure 11.1

A noter que toutes les exigences qui suivent sont conditionnées aux droits d'accès des utilisateurs.

Réf	Exigence	Test
11.8.1	Le SAE devrait permettre à un utilisateur qui est autorisé à modifier le niveau de sécurité d'un document, d'un dossier ou d'une série, de vérifier le niveau existant et les autorisations dans le déroulement normal du processus de modification.	0
11.8.2	Quand un administrateur est avisé que le niveau de sécurité d'un document a été dégradé (voir 10.13.28), il devrait pouvoir examiner le document et/ou ses métadonnées dans le déroulement normal du processus.	0
11.8.3	En cas de création d'un nouveau dossier, sous-dossier ou volume destiné à un contenant physique, le SAE devrait permettre à l'utilisateur d'imprimer une étiquette pour ce contenant physique dans le déroulement normal du processus.	0

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
	<p><i>Ceci suppose la production d'une étiquette comportant les métadonnées essentielles pour la gestion de l'entité physique, c'est-à-dire (liste non exhaustive) :</i></p> <ul style="list-style-type: none"> <li>• <i>l'intitulé ;</i></li> <li>• <i>l'identifiant système ;</i></li> <li>• <i>le code de classement ;</i></li> <li>• <i>la date d'ouverture ;</i></li> <li>• <i>le niveau de sécurité (le cas échéant) ;</i></li> <li>• <i>la localisation (l'adresse).</i></li> </ul>	
<b>11.8.4</b>	Lorsqu'un utilisateur qui supprime une information est averti de l'existence de liens (voir section 9.3), il devrait pouvoir voir ces liens et l'information liée et/ou les métadonnées dans le déroulement normal du processus.	0
<b>11.8.5</b>	Le SAE devrait permettre à un utilisateur qui masque un document d'effectuer les gestes suivants dans le déroulement normal du processus : <ul style="list-style-type: none"> <li>• masquer le document ;</li> <li>• choisir à quel niveau du plan de classement l'extrait sera classé et l'archiver ;</li> <li>• lier l'extrait à l'original ;</li> <li>• lier l'original à l'extrait.</li> </ul>	0
<b>11.8.6</b>	Quand un utilisateur déclare un document, le SAE devrait lui permettre de vérifier si le document n'a pas déjà été archivé, dans le déroulement normal du processus. <p><i>Ceci devrait être valable pour tout type de document.</i></p>	0
<b>11.8.7</b>	Le SAE devrait avertir un utilisateur qui archive un document si celui-ci a déjà été archivé, en lui indiquant son niveau de classement (série, dossier, etc.) et offrir la possibilité à l'utilisateur de poursuivre ou d'annuler la capture.	0
<b>11.8.8</b>	Quand un utilisateur capture un document, le SAE devrait lui permettre de : <ul style="list-style-type: none"> <li>• naviguer dans le plan de classement (pour trouver la série et le dossier pertinent) ;</li> <li>• regarder les métadonnées (autorisations, mots-clés, descripteurs, etc.) de toute série ou dossier ;</li> </ul> avant la fin de la capture dans le déroulement normal du processus.	0

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
<b>11.8.9</b>	<p>Quand un utilisateur a à l'écran une série, un dossier, un document, etc., dans le cadre d'une requête, en navigant dans le plan de classement ou dans un autre contexte, il devrait pouvoir effectuer directement toute opération autorisée sur cette entité, sans avoir besoin de se déplacer ailleurs dans le SAE, à savoir :</p> <ul style="list-style-type: none"><li>• l'ouvrir ;</li><li>• repérer les entités « mères » dans le plan de classement ;</li><li>• voir ses métadonnées ou l'historique des événements ;</li><li>• voir et consulter ses liens ;</li><li>• l'envoyer par messagerie ;</li><li>• changer son niveau de sécurité ;</li><li>• voir les utilisateurs et les profils qui y ont accès ;</li><li>• l'imprimer ou le restituer ;</li><li>• le masquer ;</li><li>• changer sa localisation ou le supprimer.</li></ul>	O
<b>11.8.10</b>	<p>Le SAE devrait permettre à un utilisateur de modifier le niveau de sécurité d'un document, d'un dossier ou d'une série, y compris la mise à jour de toutes les métadonnées, en une seule opération.</p>	O
<b>11.8.11</b>	<p>Si un thésaurus conforme à ISO 2788 ou ISO 5964 est intégré au SAE, le SAE devrait permettre à un utilisateur qui saisit ou met à jour un mot-clé (ou une autre métadonnée relevant du thésaurus) d'utiliser toutes les fonctions du thésaurus (termes plus larges, restreints, liés et synonymes) dans le déroulement normal du processus.</p>	O

*A noter que 8.1.18 comporte une exigence connexe pour la recherche.*

## 12. exigences liées aux métadonnées

Ce chapitre présente les exigences fonctionnelles pour les métadonnées. Le « modèle » des métadonnées de MoReq2 se trouve à l'annexe 9. La section 12.1 expose les principes et la section 12.2 énumère les exigences générales.

Dans ces spécifications, les métadonnées incluent les données d'indexation et d'autres données indispensables à un archivage efficace, notamment les droits et restrictions d'accès : voir la définition dans le glossaire. On trouvera des explications circonstanciées sur le rôle des métadonnées dans l'archivage dans la norme ISO 23081 (voir annexe 7).

### 12.1 PRINCIPES

---

#### Périmètre

Il est impossible de définir toutes les exigences relatives aux métadonnées pour tous les types de SAE. Selon les entreprises/organisations et les applications, il existe des besoins particuliers et des traditions très variées. Ainsi, certains voudront une indexation centrée sur les intitulés de comptes et les dates des transactions, tandis que d'autres se limiteront à un simple numéro d'ordre ; certains auront besoin de volumes par exercice financier, d'autres non ; certains devront contrôler l'accès pour des raisons de sécurité, d'autres gérer la propriété intellectuelle, etc.

C'est pourquoi ce chapitre de MoReq2 ne propose qu'un minimum d'exigences d'ordre générique, qui demandent à être personnalisées et développées. Elles sont liées aux listes de métadonnées spécifiques que le SAE doit être capable de capturer et de traiter. Ces métadonnées spécifiques constituent le modèle de métadonnées de MoReq2 de l'annexe 9.

### 12.2 EXIGENCES GENERALES

---

<i>Réf</i>	<i>Exigence</i>	<i>Test</i>
12.2.1	Le SAE ne doit en aucune façon limiter le nombre de métadonnées autorisées pour chaque entité (série, dossier, sous-dossier, volume, document).	P

Réf	Exigence	Test
	<i>Cette notion de limite peut varier selon l'application. Par exemple, les organisations ayant adopté un plan de classement modeste n'auront pas besoin d'autant de métadonnées que celles qui se seront dotées d'un plan de classement complexe.</i>	
12.2.2	Si le contenu d'une métadonnée peut être lié à une action dans le SAE, le SAE doit renseigner cette métadonnée au lancement de cette action.  <i>Par exemple, si le SAE stocke la date d'ouverture des dossiers, il doit renseigner cette métadonnée automatiquement à chaque ouverture de dossier plutôt que demander à un utilisateur de le faire. À noter que cette exigence générique est valable pour de nombreuses métadonnées. MoReq2 ne prétend pas identifier tous les cas de figure.</i>	P
12.2.3	Le SAE doit permettre de définir différents jeux de métadonnées pour différents types de documents au moment de la configuration.  <i>Par exemple, les métadonnées requises seront :</i> <ul style="list-style-type: none"> <li>• pour les factures, des numéros de compte ;</li> <li>• pour le courrier, des champs destinataires multi-valeurs ;</li> <li>• pour les documents numérisés, des données relatives à la numérisation et à l'indexation.</li> </ul>	O
12.2.4	Le SAE doit permettre à l'administrateur de préciser lors de la configuration si une métadonnée est obligatoire ou facultative.	O
12.2.5	Le SAE doit accepter au minimum les formats de métadonnées suivants : <ul style="list-style-type: none"> <li>• alphabétique,</li> <li>• alphanumérique,</li> <li>• numérique,</li> <li>• date,</li> <li>• logique (OUI/NON, VRAIX/FAUX, etc.).</li> </ul>	O
12.2.6	Le SAE devrait accepter des formats de métadonnées définis par l'administrateur sur la base d'une combinaison des formats du point 12.2.5.  <i>Par exemple, un dossier peut avoir un identifiant du type nnnnn/aa-n.</i>	O
12.2.7	Le SAE doit accepter tous les formats de date définis dans ISO 8601.	O
12.2.8	Lors de la configuration, le SAE doit permettre de préciser la source des données pour chaque métadonnée.  <i>Les sources possibles sont décrites aux points 12.2.9, 12.2.10, 12.2.11 et 12.2.12.</i>	O
12.2.9	Le SAE doit permettre à un administrateur de préciser quelles métadonnées doivent être saisies et mises à jour manuellement ou sélectionnées dans un vocabulaire contrôlé.	O

Réf	Exigence	Test
12.2.10	<p>Le SAE devrait permettre que certaines métadonnées soient, par défaut, héritées automatiquement à partir du niveau immédiatement supérieur du plan de classement.</p> <p><i>Par exemple, pour un volume, la valeur de certaines métadonnées doit être héritée de son sous-dossier « père » ; et pour un document, la valeur de certaines métadonnées peut être héritée du volume où il est classé.</i></p>	0
12.2.11	<p>Le SAE devrait permettre que certaines métadonnées soient obtenues à partir de tables de conversion ou en interrogeant d'autres applications.</p> <p><i>Par exemple, le SAE pourrait fournir les noms et les codes postaux à une application d'adressage qui en retour fournit un nom de rue comme métadonnée.</i></p>	0
12.2.12	<p>Quand les métadonnées sont renseignées à partir de tables de conversion, si le choix d'une valeur en exclut d'autres, cela doit être pris en compte dans les tables suivantes proposées à l'utilisateur.</p>	0
12.2.13	<p>Le SAE devrait être capable de gérer des métadonnées en provenance :</p> <ul style="list-style-type: none"> <li>• d'une application de production de documents (voir 6.1.12) ;</li> <li>• d'un système d'exploitation ;</li> <li>• d'un logiciel de réseau ;</li> <li>• de l'utilisateur, au moment de la capture ou de la déclaration ;</li> <li>• de règles de production de métadonnées par le système au moment de l'archivage, définies au moment de la configuration.</li> </ul>	0
12.2.14	<p>Le SAE doit être capable de valider des métadonnées saisies par les utilisateurs ou importées. La validation doit utiliser au minimum les mécanismes suivants :</p> <ul style="list-style-type: none"> <li>• format des contenus ;</li> <li>• plage de valeurs ;</li> <li>• validation par rapport à une liste de valeurs gérée par un administrateur.</li> </ul> <p><i>Exemple de validation du format : tous les contenus sont numériques ou au format date (selon 12.2.5.). Exemple de validation par rapport à un ensemble de valeurs : les contenus sont compris entre le 1er janvier 1999 et le 31 décembre 2001. Exemple de validation par rapport à une liste de valeurs : vérification que le nom exporté figure sur une liste.</i></p>	0
12.2.15	<p>Le SAE doit être capable de valider des métadonnées en interrogeant d'autres applications (un système de ressources humaines en vérifiant si un matricule a été attribué, ou une base de données de codes postaux) ou en utilisant une table de conversion interne.</p>	0
12.2.16	<p>Le SAE doit permettre à un administrateur de paramétrer la validation pour chaque métadonnée (voir 12.2.14 et 12.2.15).</p>	0

Réf	Exigence	Test
	La validation dépend du type de métadonnée : les dates demanderont une validation de format alors que les descriptions n'ont pas besoin d'être validées.	
12.2.17	<p>Pour les métadonnées saisies manuellement, le SAE devrait permettre à un administrateur de les configurer pour qu'elles acceptent les valeurs suivantes :</p> <ul style="list-style-type: none"> <li>• valeurs par défaut définies par un utilisateur ;</li> <li>• une valeur fixe par défaut ;</li> <li>• la date du jour (pour les métadonnées date) ;</li> <li>• non renseigné.</li> </ul> <p>On peut admettre également d'autres types de saisie.</p> <p><i>La valeur par défaut apparaît systématiquement pour toute entrée jusqu'à ce qu'elle soit modifiée par un utilisateur. Une fois modifiée, c'est cette nouvelle valeur qui est proposée par défaut. Elle devrait être proposée jusqu'à la fin de la session ou, mieux, d'une session à l'autre. Ceci vaut pour toutes les entités possédant des métadonnées saisies par l'utilisateur.</i></p>	O
12.2.18	Le SAE devrait permettre une configuration telle que toute métadonnée soit interrogeable lors d'une recherche en texte intégral.	O
12.2.19	<p>Lorsqu'une métadonnée est stockée dans un format date, le SAE devrait permettre une recherche sur la valeur de la date.</p> <p><i>Par exemple, le SAE devrait permettre les recherches sur une série de dates. Il ne suffit pas que la date soit stockée dans un champ texte.</i></p>	O
12.2.20	Lorsqu'une métadonnée est stockée dans un format numérique, le SAE devrait permettre une recherche sur la valeur du nombre.	O
12.2.21	Le SAE doit permettre aux administrateurs de restreindre le droit de modifier les valeurs des métadonnées (voir le modèle de contrôle d'accès section 13.4).	O
12.2.22	<p>Le SAE doit permettre à un administrateur de reconfigurer le modèle de métadonnées et tracer l'opération dans l'historique des événements.</p> <p><i>Par exemple, on peut avoir besoin d'ajouter une métadonnée « identifiant du département » à certains types de documents à la suite d'une réorganisation.</i></p>	P
12.2.23	Le SAE doit permettre de paramétrer les métadonnées lors de la configuration de sorte que les valeurs issues d'autres logiciels applicatifs, du système d'exploitation ou du SAE (par exemple, la messagerie électronique) ne puissent être modifiées par l'utilisateur après la capture.	O
12.2.24	Le SAE doit permettre de paramétrer les métadonnées lors de la configuration de sorte que, une fois saisies, l'utilisateur ne puisse plus les modifier.	O

## 13. Modèle de référence

Ce chapitre fournit le modèle de référence pour l'ensemble des exigences de MoReq2.

Les quatre sections sont :

- le glossaire (section 13.1) ;
- le modèle de relations entre les entités (section 13.2) ;
- l'explication des relations entre les entités (section 13.3) ;
- le modèle de contrôle d'accès (section 13.4).

### 13.1 GLOSSAIRE

---

Ce glossaire définit les termes essentiels utilisés par MoReq2<sup>1</sup>.

Certaines définitions importantes sont tirées ou adaptées des glossaires des publications citées en référence dans l'annexe 1 ; ces sources sont signalées après chaque définition.

Les mots définis dans le glossaire sont *en italique*.

#### **administrateur (administrator)**

Personne responsable au quotidien de l'application de la politique d'archivage au sein de l'entreprise/organisation.

Note : il s'agit d'une simplification. Dans les grandes structures, les tâches dévolues ici aux administrateurs se répartissent souvent entre plusieurs fonctions : records manager, gestionnaire des documents, archiviste, etc.

#### **authenticité (authenticity)**

(dans le contexte de l'archivage uniquement) Qualité de ce qui est original.

Source : adapté et résumé de la définition d'"authenticité archivistique" dans le glossaire UBC-MAS (annexe 1)

Note : un document archivé est authentique s'il peut prouver :

- a) qu'il est ce qu'il prétend être ;
- b) qu'il a été créé ou envoyé par la personne qui prétend l'avoir créé ou envoyé, et

---

<sup>1</sup> Note du traducteur : le glossaire est présenté dans l'ordre alphabétique des termes français avec le terme anglais original entre parenthèses.

c) qu'il a été créé ou envoyé à la date prétendue".

Source : ISO 15489.

Note : pour un *document archivé*, cette qualité implique que le document soit ce qu'il prétend être ; elle ne vise pas la fiabilité du contenu du document en tant que tel.

### **capturer (capture, verb)**

(1) Action d'enregistrer ou de sauvegarder une instance particulière d'un objet numérique (source: InterPARES 2 Projet de base de données terminologique).

(2) Sauvegarder une information dans un système informatique.

Note : dans MoReq2, la capture des *documents à archiver* désigne l'ensemble des processus conduisant à l'archivage d'un document dans le SAE, c'est-à-dire : enregistrement, classement, ajout de métadonnées et fixation des contenus du document source. Le mot désigne aussi une entrée dans le SAE avec le stockage d'informations complémentaires telles que les métadonnées.

### **classement (classification)**

Dans l'archivage, identification et ordonnancement systématiques des activités métier et/ou des *documents à archiver* en catégories selon une structure logique prédéfinie, des méthodes et des règles concrétisées dans un plan de classement.

Source : ISO 15489 (voir annexe 7).

### **clôture (close, verb)**

Action de modifier les attributs d'un *dossier, sous-dossier ou volume* de sorte qu'on ne puisse plus y ajouter de *documents*.

### **clos (closed)**

Qualificatif d'un *dossier, sous-dossier ou volume* qui n'est plus ouvert et ne peut donc accepter de nouveaux documents.

### **CMS (Content Management System - CMS)**

Système de gestion de contenu (SGC).

### **code de classement (classification code)**

Identifiant attribué à chaque série du plan de classement. Au sein de chaque série, les codes de classement des séries filles sont uniques.

### **composant (component)**

Train de bit indépendant qui, seul ou combiné à d'autres, constitue un document (archivable ou non).

Note : le mot n'est pas d'usage courant.

Note : l'expression "train de bit indépendant" équivaut à ce qu'on appelle couramment un "fichier" en informatique<sup>1</sup>. Le concept fondamental est qu'un composant fait partie intégrante du contenu du document archivé, même s'il peut être stocké et géré séparément.

Note : un composant sera par exemple :

- Un document HTML et les images JPEG qui constituent une page web ;
- Un document bureautique, texte et tableau, composé d'un document texte avec un lien embarqué (hyperlien) vers un tableur ;

Note : les composants doivent être distincts et séparés les uns des autres. Si un document texte contient un tableau incorporé (par opposition à un hyperlien vers le tableur), le tableau ne doit pas être considéré comme un composant ; dans ce cas, le document texte incluant le tableau ne constitue qu'un seul et même document.

Note : un courriel avec ses pièces jointes peut être un seul composant ou plusieurs, ou même plusieurs documents distincts, en fonction du format des données.

- Si le message est stocké dans un format qui inclut le corps du message et les pièces jointes, il n'y a qu'un composant.
- Si les pièces jointes sont stockées séparément du corps du message mais avec un lien, chaque pièce jointe, de même que le corps du message, est un composant.
- Si les pièces jointes sont stockées séparément du corps du message sans y être reliées, chaque pièce jointe ainsi que le message constituent des documents distincts ; les bonnes pratiques suggèrent de relier ces documents manuellement.

#### conversion de fichier, conversion (rendition)

Représentation d'un document ou de ses *composants* utilisant un ou des *formats de fichier* différent(s) du ou des format(s) natif(s).

Note : les conversions visent à préserver les documents électroniques, en réduisant le risque de perte d'accès à leur contenu dans le temps. Ainsi, les documents créés dans un format propriétaire peuvent être archivés et stockés dans un format normé du type PDF/A ou XML.

La conversion d'un document sous-entend la conversion de tout ou partie de ses *composants*. Après la conversion, le document n'aura pas nécessairement le même nombre de composants. Par exemple, un document constitué de 30 composants dont 10 images GIF pourra être converti de plusieurs façons, notamment :

- Conversion du document au format PDF/A : dans ce cas le document initial a 30 composants et sa conversion un seul ;
- Simple conversion des composants GIF au format JPEG : dans ce cas le document et sa conversion ont l'un et l'autre 30 composants ; en outre certains objets de la conversion doivent être modifiés pour intégrer la référence aux nouvelles images JPEG.

Note : le mot « rendition » avait un autre sens dans la première version de MoReq<sup>2</sup>.

---

<sup>1</sup> Note du traducteur : le mot anglais pour fichier étant « file », il a été évité dans la version anglaise pour éviter la confusion avec le mot dossier ("file" également).

<sup>2</sup> Note du traducteur : dans la première version de MoReq, rendition avait le sens de présentation (en français restitution) de MoReq2.

### convertir (render)

Action de réaliser une *conversion de fichier*.

### Destruction (destruction)

Opération consistant à éliminer les documents archivés sans aucune possibilité de reconstitution.

Source : ISO 15489 (voir annexe 7).

Note : selon la configuration retenue, la destruction sera assimilée à la suppression ou non.

Note : la réécriture des données ou d'autres mesures de ce type ne sont pas prévues. Des mesures de sécurité supplémentaires peuvent être mises en œuvre mais MoReq2 ne l'exige pas.

### document (document, noun)<sup>1</sup>

Information enregistrée ou objet qui peut être traité comme une unité.

Source: ISO 15489 (voir annexe 7).

Note : un document peut être sur papier, microforme, support magnétique ou autre support numérique. Il peut comporter toute combinaison de texte, données, graphiques, son, images animées, etc. Un document unique peut être constitué d'un ou plusieurs *composants*.

Note : les simples documents présentent plusieurs différences importantes par rapport aux *documents à archiver ou archivés*. MoReq2 désigne par document une information qui n'a pas été capturée dans le système d'archivage, c'est-à-dire classée, enregistrée et figée. Le seul fait de capturer ne confère pas la qualité de *document archivé*. À noter cependant qu'un certain nombre de documents capturés sont archivés.

### document à archiver, document archivé (record, noun)

Documents créés, reçus ou préservés à titre de preuve et d'information par une personne physique ou morale dans l'exercice de ses obligations légales ou la conduite de son activité.

Source: ISO 15489 (voir annexe 7).

Note : les définitions nationales sont aussi recevables.

Note : un document archivé peut comporter plusieurs *pièces* (cas des pièces jointes), et peut se présenter sous n'importe quel support et format. Il peut donc être constitué d'un ou plusieurs composants. Outre son contenu informatif, un document archivé devrait inclure une information contextuelle et, le cas échéant, l'information de structure (description des composants, etc.). Une des caractéristiques fondamentales du document archivé est qu'il ne peut plus être modifié.

Note : un SAE peut gérer à la fois l'archivage électronique et l'archivage physique.

### document archivé hors SAE (physical record)

---

<sup>1</sup> Note du traducteur : dans la traduction française, le mot document désigne parfois les documents archivés, quand le contexte est sans ambiguïté. ailleurs, le mot anglais « document » est également rendu par le mot français « pièce » - cas d'un document constitué de plusieurs pièces (record made of several documents).

*Document archivé* stocké sur un support à l'extérieur du SAE, de sorte que le document n'est pas directement géré par le SAE.

Exemples : tous dossiers papier, microformes, documents électroniques stockés sur des supports amovibles dès lors que les documents ne sont pas gérés directement par le SAE.

#### **document électronique (electronic document)**

Un *document* qui se présente sous la forme électronique.

Note : l'expression *document électronique* n'est pas limitée aux documents texte issus des outils de traitement de texte. Elle inclut les courriels, les tableaux, les graphiques et les images, les documents HTML/XML, multimédia et les documents composites, etc.

#### **document électronique à archiver ou archivé (electronic record)**

Un document à archiver ou archivé sous forme électronique.

Note : la forme électronique peut soit être native (production d'une application informatique), soit résulter d'une opération de numérisation, notamment d'un scan.

#### **document vital (vital record)**

Un document à archiver ou archivé essentiel au fonctionnement et/ou à la survie d'une entreprise/organisation en cas de sinistre.

#### **dossier (file, noun)**

Ensemble organisé de documents traitant du même sujet ou procédant de la même activité ou opération.

Source : résumé et adapté de ISAD(G) (voir annexe 7)<sup>1</sup>.

#### **dossier non sériel (non case file)**

Tout dossier qui n'est pas un *dossier sériel*.

#### **dossier papier (paper file)**

Type de dossier physique.

Note : les enveloppes, les boîtes d'archives, les reliures sont des exemples de dossiers papier.

#### **dossier physique (physical file)**

Moyen matériel de maintenir physiquement des documents.

Source : adapté des spécifications fonctionnelles PRO (voir annexe 1).

#### **dossier sériel (case file)**

---

<sup>1</sup> Note du traducteur: la version anglaise de MoReq2 utilise *component* pour désigner les fichiers informatiques (« file ») afin de les distinguer des dossiers (« file » également). Le mot *file* est traduit par dossier et le mot *component* par composant.

Un dossier traçant une ou plusieurs opérations effectuées totalement ou partiellement de manière structurée ou semi-structurée, et résultant d'un processus ou d'une action précise.

Note : il n'existe pas de définition universelle de ces termes ni de la distinction entre les dossiers sériels et les autres types de dossiers gérés par un SAE. Il s'agit d'une définition *ad hoc* qui vise à faciliter la compréhension de MoReq2 ; son utilisation dans d'autres environnements n'est pas garantie.

Note : les pièces d'un dossier sériel peuvent être structurées ou non structurées. La caractéristique principale d'un dossier sériel est qu'il résulte d'un processus qui est structuré, au moins en partie, et répétitif. Exemples :

- demandes de permis ;
- réclamations courantes ;
- enquête sur un incident ;
- contrôle régulier.

Note : les autres caractéristiques d'un dossier sériel sont que, en général :

- la structure de leur contenu est prédictible ;
- ils sont produits en nombre ;
- ils sont structurés ou semi-structurés ;
- ils sont gérés par un processus connu et prédéterminé ;
- ils doivent être conservés pendant des durées imposées par la réglementation ;
- ils peuvent être ouverts et clos par des gestionnaires, des utilisateurs finaux ou des systèmes informatiques sans intervention du management.

### électronique (electronic)

Dans ces spécifications, le mot "électronique" est utilisé dans le sens de "numérique".

Note : des enregistrements analogiques, bien qu'électroniques à certains égards, ne sont pas "électroniques" dans l'optique de MoReq2 dans la mesure où ils ne peuvent être stockés dans un système informatique sans être convertis au format numérique. C'est pourquoi, ce glossaire assimile les enregistrements analogiques à des documents physiques.

### enregistrement (registration)<sup>1</sup>

Action d'affecter un identifiant unique à un document au moment de son archivage.

Source : ISO 15489 (voir annexe 7).

Note : MoReq2 considère l'enregistrement comme une part du processus de *capture*.

### exporter (export, verb)

Opération consistant à effectuer une copie des *documents électroniques archivés*, avec leurs *métadonnées*, pour un autre système.

---

<sup>1</sup> Note du traducteur : enregistrement traduit également dans ce texte le mot anglais « recording », dans l'expression « analogue recordings » : enregistrements analogiques.

Note : les documents exportés restent dans le SAE, à l'inverse du *transfert*.

#### extrait (redaction, noun)

(pour un *document archivé*) Copie d'un *document* ayant subi des modifications dans le but de retirer ou masquer des données, jamais pour en modifier significativement le contenu<sup>1</sup>.

Source : définition d' "instance" dans les spécifications fonctionnelles PRO (voir annexe 1).

Note : les modifications résultent en général d'une contrainte de non divulgation de l'information. Ainsi, un *document* ne sera accessible qu'après masquage ou retrait des noms de personnes ; on crée alors un extrait du document où les noms sont illisibles. Ce processus est parfois appelé masquage.

#### format de fichier (file format)

Structure interne et/ou encodage d'un *document* ou d'un *composant*, permettant de lui donner une forme accessible à l'homme.

Exemples :

- HTML v3.2 (format de fichier pour pages web) ;
- PDF/A v1 (format d'archivage pour les documents portables) ;
- TXT (format plein texte ASCII) ;
- XML v1.0 (format pour un langage de balisage extensible lui-même basé sur du plein texte ASCII).
- Divers formats propriétaires issus des applications ou suites bureautiques.

#### GED (EDMS)

Système de Gestion Électronique de Document.

Application informatique dédiée à la gestion des documents et de leur cycle de vie.

Source : IEC 82045-1 Gestion des Documents.

Note : toutes les fonctionnalités d'une GED ne sont pas exigées par ces spécifications. Ceci dit, un système de GED est souvent intégré à un système d'archivage. Voir le détail en section 10.3.

#### gel (disposal hold)

Décision interdisant la *destruction* ou le *transfert* des *documents archivés*.

#### gestionnaire de dossiers sériels (case worker)

Un *utilisateur* qui gère des *dossiers sériels*.

#### groupe (group, noun)

Ensemble d'utilisateurs.

---

<sup>1</sup> Note du traducteur : le texte anglais précise que ce terme de « redaction » remplace le terme « extract » de la première version de MoReq. Le texte français utilise « extrait » dans les deux versions.

Note : les utilisateurs d'un groupe n'ont pas nécessairement le même *profil*. Le groupe peut être défini sur la base d'une unité fonctionnelle telle qu'une direction (où les profils sont par nature variés), ou sur la base de l'appartenance à une équipe virtuelle transverse à l'organisation, par exemple les responsables d'achat (parfois seulement les personnes ayant tel profil), etc.

#### **groupe de documents (aggregation)**

(dans MoReq2 uniquement) Une série, un dossier, un sous-dossier ou un volume.

#### **groupe utilisateur (user group)**

Voir *groupe*.

#### **habilitation (security clearance)**

Un ou plusieurs termes associés à un *utilisateur* pour préciser les *niveaux de sécurité* auxquels il peut accéder.

#### **historique des événements (audit trail)**

Données sur les opérations qui impactent ou modifient les entités (autrement dit métadonnées), suffisamment détaillées pour permettre de reconstituer l'activité passée.

Note : l'historique consiste en une ou plusieurs listes ou en une base de données chronologique. Ces listes peuvent être manuelles (pour les opérations manuelles) mais MoReq2 met l'accent sur leur production par un système informatique (transactions informatiques).

#### **import par lots (bulk importing)**

Processus de capture d'un lot de documents électroniques, *a priori* en provenance d'une autre application, avec tout ou partie de leurs métadonnées.

#### **masquer (redact)**

Action de cacher les données sensibles d'un *document archivé*.

Note : on peut recouvrir les noms avec des rectangles opaques, etc. (équivalent électronique du fait de rayer les documents papier à l'encre), oblitérer l'information avec des méthodes plus sécurisées ou supprimer certaines pages.

Note : le document électronique original n'est en aucun cas altéré. Le masquage est effectué sur une copie du document ; cette copie est appelée *extrait*.

#### **métadonnées (metadata)**

(Dans le contexte de l'archivage) Données décrivant le contexte, le contenu et la structure des documents archivés et leur gestion dans le temps.

Source: ISO 15489 (voir annexe 7).

Note : certains modèles reposent sur une conception différente des métadonnées, par exemple en considérant les données d'historiques des événements comme des métadonnées à part entière. Ces approches sont valables dans certains contextes mais ne permettent pas de préciser les fonctionnalités du système et ne sont donc pas retenues ici.

### métadonnées-témoins (metadata stub)

Choix de métadonnées conservées après la destruction ou le transfert d'un objet archivé, comme preuve que celui-ci a bien existé et a été détruit ou transféré dans les règles.

### moment de la configuration (configuration time)

Étape, dans la vie d'un SAE, correspondant à son installation et à la définition des paramètres.

### mot-clé (keyword)

Métadonnée facultative pour décrire les séries, dossiers, sous-dossiers et documents (pas les volumes).

Note : les bonnes pratiques veulent que les mots-clés soient tirés ou validés à l'aide d'une liste d'autorité, ou extraits automatiquement par le SAE, mais ce n'est pas obligatoire.

### niveau de sécurité (security category)

Un ou plusieurs termes associés à un *document archivé* ou à un *groupe de documents* pour réglementer son accès.

Note : les niveaux de sécurité sont généralement définis au niveau de l'organisation ou au plan national. A titre d'exemple, les administrations gouvernementales européennes utilisent : « Secret Défense », « Secret », « Confidentiel », « Restreint », « Non classifié ». S'y ajoutent parfois d'autres termes tels que « Restreint à l'Union européenne occidentale » ou « Personnel ».

Note : tout le monde n'utilise pas cette expression. MoReq2 l'a retenue plutôt que « classification », fréquemment utilisé dans le monde de la sécurité, pour éviter la confusion avec « classification » utilisé au sens de *classement* dans le monde documentaire.

### numérique (digital)

Qualificatif des informations construites à l'aide de digits ou de nombres et non à l'aide de grandeurs continues.

Note : ce terme n'est pas utilisé par MoReq2 pour qualifier les documents. Bien que "document numérique" soit plus précis que "document électronique", l'expression est très peu utilisée. *Voir électronique.*

### ouverture (open, verb)

Processus consistant à créer un nouveau *dossier*, *sous-dossier* ou *volume* susceptible de recevoir de nouveaux documents.

### ouvert (open, adjective)

Qualificatif d'un *dossier*, *sous-dossier* ou *volume* qui n'est pas encore *clos* et qui est donc susceptible de recevoir de nouveaux documents.

### PDF (PDF)

Portable Document Format, *format de fichier* initialement destiné à la représentation de l'information en deux dimensions.

Note : à ce jour, ce format, très largement utilisé, appartient à la société Adobe mais une récente version du format (v1.7) est examinée en vue d'une norme internationale (ISO/DIS 32000)<sup>1</sup>. La présence de PDF dans ce glossaire ne vaut pas caution. L'extension du format pour une représentation en trois dimensions est à l'étude.

#### PDF/A (PDF/A)

Déclinaison du format PDF dédiée à l'archivage, régie par les normes ISO 19005.

#### pièce

voir document.

#### plan de classement (classification scheme)

(dans MoReq2) Organisation hiérarchique des séries, dossiers, sous-dossiers, volumes et documents.

#### profil (role)

Ensemble des autorisations fonctionnelles attribuées à un ensemble prédéfini d'*utilisateurs*.

Source : spécifications fonctionnelles PRO (voir annexe 1).

#### profil d'administration (administrative role)

Ensemble de droits dévolus aux *utilisateurs* autorisés à effectuer des opérations d'administration.

Note: MoReq2 utilise également ce terme pour désigner les personnes bénéficiant de ces droits.

#### profil utilisateur (user role)

Ensemble d'autorisations allouées aux *utilisateurs* ayant le droit d'effectuer des opérations sur les *documents archivés*.

Un utilisateur peut avoir plusieurs *profils* mais il n'a qu'un *rôle*.

Note : MoReq2 utilise aussi ce terme pour désigner les personnes autorisées.

#### propriétaire (owner)

Personne ou rôle responsable d'un *document archivé* ou d'un *groupe de documents*.

Note : c'est le sens retenu par MoReq2 ; le propriétaire légal d'un document archivé est l'entreprise/organisation qui détient le document.

Note : voir aussi *responsable du stockage*

#### règles de conservation/destruction (retention and disposition schedule)

Document de référence qui définit, pour un ensemble de documents à archiver, les durées de conservation et les actions de sort final autorisées.

---

<sup>1</sup> Note du traduction : la norme a été publiée ; il s'agit de la norme ISO 32000-1.

Source : adapté du glossaire archivistique des Archives nationales d'Australie.

Note : "règles de conservation/destruction" correspond à "tableau de conservation" dans la première version de MoReq.

#### rendez-vous (rendezvous)

Étape d'un workflow où deux opérations ou plus, exécutées en parallèle, convergent en un seul point de contrôle.

Source : terminologie et glossaire de la Workflow Management Coalition, édition 3.0.

#### répertoire (repertory)

Liste des titres des *dossiers* sous chaque branche du plan de classement.

#### responsable du stockage (custodian)

(d'un document ou d'un groupe) personne ou service ayant la charge des *documents archivés*.

#### restitution (presentation)

Présentation d'un *document archivé électroniquement* fournie par le SAE à un *utilisateur*.

Note : ce sera un affichage à l'écran, une impression ou un objet audiovisuel ou multimédia.

Note : la nature exacte de la restitution peut être affectée par l'environnement matériel et logiciel. Les différentes restitutions d'un même document peuvent varier en termes de polices de caractères, fins de ligne et pagination, résolution, profondeur, espace couleur, etc. En général, ces différences sont acceptables. Mais parfois, leurs conséquences éventuelles méritent d'être prises en considération ; ces questions dépassent le cadre de ces spécifications.

#### rôle (profile)

Ensemble des autorisations allouées à un utilisateur, un groupe ou un profil.

#### rôle utilisateur (user profile)

Rôle d'un utilisateur.

#### SAE (ERMS)

Système d'Archivage Électronique

Note : les SAE présentent plusieurs différences importantes par rapport aux système de GED. Voir le détail section 10.3.

#### série (class, noun)

(dans MoReq2 seulement) Partie d'un *plan de classement* partant de n'importe quel point de l'arborescence et englobant tous les dossiers en dessous de ce point.

Note : cette définition correspond, en documentation, à une « division primaire », un « groupe » ou une « série » (subdivision, sous-groupe, sous-série, etc.) à n'importe quel niveau du plan de classement.

Note : dans MoReq2, série peut aussi désigner l'ensemble des documents rattachés à une série.

### sort final (disposition)

Ensemble des opérations de mise en œuvre de la conservation définitive, de la *destruction* ou du *transfert* des *documents archivés*, conformément aux règles de conservation/destruction.

Source : ISO 15489 (voir annexe 7).

### sous-dossier (sub-file)

Subdivision intellectuelle d'un *dossier*.

Note : les sous-dossiers sont plus spécialement utilisés pour la gestion des dossiers sériels. Dans ce cas, chaque sous-dossier est destiné à conserver un ou plusieurs types de documents entrant dans la composition du dossier, par exemple : "factures", "évaluations", "correspondance". Cette utilisation peut être étendue aux dossiers non sériels.

### Système de Gestion de Contenu (SGC)

Voir CMS

### témoins

voir métadonnées-témoins.

### transférer (transfer, verb)

Action de faire passer des *dossiers électroniques*, avec leurs *métadonnées*, à un autre système.

Source : adapté des spécifications fonctionnelles PRO (Annexe 1, référence [2]).

Note : les dossiers sont souvent transférés par groupes au sein d'une *série* du *plan de classement* quand il s'agit d'un versement à un centre d'archives pour conservation définitive.

Note : voir aussi *export*.

### type de document (document type)

Désignation de *documents* présentant les mêmes caractéristiques.

Exemples de documents avec la même présentation, le même contenu, les mêmes règles de conservation/destruction, et/ou les mêmes *métadonnées* :

- formulaire de candidature ;
- correspondance (lettres, fax, notes, etc.) ;
- curriculum vitae ;
- courriels ;
- facture ;
- rapport médical ;
- page web.

Note : les courriels sont distingués ici de la correspondance dans la mesure où les métadonnées peuvent être différentes, mais ce n'est pas systématique.

Note : chaque entreprise/organisation doit définir ses types de documents selon ses métiers ; la liste ci-dessus n'est qu'un exemple.

#### type de document archivé (record type)

Désignation d'un *document à archiver ou archivé* à partir de son *type de document*.

#### utilisateur (user)

Toute personne qui utilise le *SAE*.

Note : ce sont notamment les administrateurs, les secrétaires, les collaborateurs ou des personnes extérieures telles que les auditeurs.

Note : un utilisateur peut avoir plusieurs *profils* et appartenir à des *groupes*.

#### utilisateur autorisé (authorised user)

Un *utilisateur* qui a le droit d'effectuer telle ou telle opération.

Note : le détail dépend du contexte. Les différents utilisateurs bénéficient d'autorisations différentes. MoReq2 ne se prononce pas sur les critères d'affectation de ces autorisations. Le droit d'effectuer telle ou telle opération est accordé à l'utilisateur par l'entreprise/organisation, en vertu de sa politique et de ses exigences métier.

#### version (version)

(pour un *document*) État d'un document à une certaine étape de son développement.

Source : spécifications fonctionnelles PRO (voir annexe 1).

Note : version désigne l'un des états intermédiaires du *document*, ou le document final. Il peut exister plusieurs versions du document final (ex : un manuel technique). La version peut aussi correspondre à une traduction. En revanche, le *document archivé* n'existe qu'en une seule version ; voir aussi *extrait*.

#### volume (volume)

Subdivision d'un *sous-dossier*.

Note : ces subdivisions sont créées pour améliorer la maniabilité du contenu des sous-dossiers, grâce à de petites unités faciles à gérer. Elles sont mécaniques (basées sur un nombre de documents, des numéros ou un laps de temps) plutôt qu'intellectuelles.

## 13.2 MODELE RELATIONNEL DES ENTITES

---

Cette section reprend une partie de la section 2.3, pour faciliter la lecture.

Elle contient un modèle des relations entre entités qui peut aider à comprendre l'ensemble des spécifications. La section 13.3 contient une description et une explication du modèle.

Le modèle des relations entre entités est présenté dans la figure 13.3. Il est important de noter qu'il ne décrit pas les structures réellement présentes dans le SAE. Il donne une vue théorique des entités associées aux documents archivés. Un SAE utilise ces relations pour créer un fonctionnement correspondant à ce schéma. Voir la section 2.2 pour plus de détail.

La relation entre les dossiers, volumes, documents et autres entités essentielles sont décrites dans ce modèle des relations entre entités. C'est une représentation formelle d'une sélection de structures visant à décrire le fonctionnement d'un SAE.

Dans le schéma, les entités - dossiers, documents, etc. - sont représentées par des rectangles. Les connecteurs représentent les relations entre ces entités. Chaque relation est légendée au milieu du trait ; la légende se lit dans le sens de la flèche. Le nombre indiqué à la fin de la relation correspond au nombre d'occurrences (*stricto sensu* la cardinalité) ; ce nombre est explicité en bas du schéma. Exemple : la figure 13.1 signifie « un document est constitué d'un ou plusieurs composants » (noter la direction de la flèche).

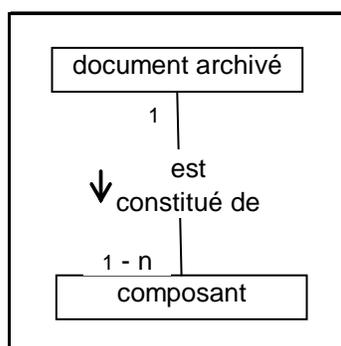


Figure 13.1

Un arc de cercle traversant deux relations ou plus indique que ces relations, pour une instance donnée, sont exclusives. Exemple : l'arc de cercle de la figure 13.2 signifie « un document est archivé soit dans un volume soit dans un sous-dossier mais pas dans les deux ».

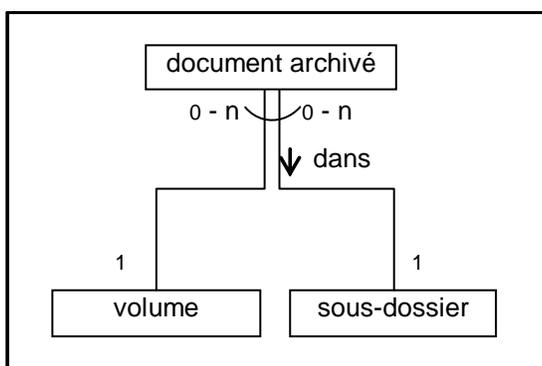


Figure 13.2

A noter que l'entité série est reliée à elle-même par la relation « est constitué de ». Cette relation désigne la relation entre les séries au sein d'un plan de classement hiérarchique où une série peut être subdivisée en une ou plusieurs autres séries. Si cette relation (appelée parfois récursive) est supprimée, le modèle s'applique également à des relations non hiérarchiques.



## 13.3 DESCRIPTION DES RELATIONS ENTRE ENTITES

---

La figure 13.3 montre un modèle simplifié ; il ne prétend pas représenter toutes les entités ou relations possibles. Il ne montre que les plus significatives pour un SAE. C'est pourquoi les utilisateurs, les rôles, etc. n'y figurent pas.

Les pages qui suivent donnent une explication des entités du schéma avec leurs relations.

### Plan de classement

Pour appliquer les principes du records management, une entreprise/organisation doit avoir au moins un plan de classement qui restitue la structure de classement (une organisation hiérarchique) de tout ou partie de ses services. Un plan de classement comporte plusieurs séries.

### Série

On peut voir les plans de classement hiérarchiques comme la hiérarchie constituée de X séries comme les branches d'un arbre. Chaque série est reliée à la hiérarchie à un certain niveau ; elle peut recouvrir plusieurs branches et contenir de plus petites séries. Plusieurs séries peuvent démarrer au même niveau, mais une série démarre à un seul niveau. Comme le précise la relation « exclusive », une série peut :

- être composées de séries, ou
- contenir des dossiers, ou
- conserver des documents ;

mais les combinaisons ne sont pas autorisées.

### Dossier

Les dossiers se trouvent dans les séries, à tout niveau de la hiérarchie, mais seulement dans les séries qui ne contiennent pas d'autres séries. Comme le précise la relation « exclusive », un dossier peut :

- être divisé en sous-dossiers, ou
- être divisé en volumes, ou
- conserver des documents ;

mais les combinaisons ne sont pas autorisées.

### Sous-dossier

Un dossier peut être subdivisé en sous-dossiers (l'existence de sous-dossiers est validée par une option de configuration). En fait, certains dossiers n'ont pas de sous-dossiers. Quand il n'y a qu'un sous-dossier, le concept de sous-dossier est transparent pour les utilisateurs. Les sous-dossiers sont souvent utilisés pour les dossiers sériels. Comme le précise la relation « exclusive », un sous-dossier peut :

- être divisé en volumes, ou
- conserver des documents ;

mais les combinaisons ne sont pas autorisées.

## Volume

Un sous-dossier peut être subdivisé en volumes (l'existence de volumes est validée par une option de configuration) selon certains critères. En réalité, peu de sous-dossiers sont divisés en volumes. Quand il n'y a qu'un volume, le concept de volume est transparent pour les utilisateurs. Les critères sont liés à la taille ou au nombre des documents, à des opérations ou à des laps de temps. Cette pratique vient de la gestion des dossiers papier et vise à rendre leur taille et leur poids acceptables. Pour l'électronique, il s'agit, le cas échéant, de limiter les dossiers à une taille adaptée à la révision, au transfert, etc.

Quand un dossier ne comprend qu'un seul sous-dossier, l'utilisateur peut penser que ses volumes relèvent du dossier plutôt que du sous-dossier.

En fait, les termes dossier, sous-dossier et volume sont parfois interchangeables ou employés de manière floue - en raison de cette exigence de transparence. Ainsi, un utilisateur demandera « un dossier » plutôt que d'utiliser le terme « volume » plus précis. On le voit particulièrement dans le cas d'un dossier physique constitué d'un seul sous-dossier en un volume. Dans ce cas, bien que le dossier, *stricto sensu*, soit constitué d'un sous-dossier ne comportant lui-même qu'un volume, le sous-dossier et le volume ne seront pas identifiés en tant que tels (le plus souvent, le titre ne sera correct qu'à partir du second sous-dossier ou volume).

## Règle de conservation/destruction

Une règle de conservation/destruction fixe les règles de conservation et de sort final des documents archivés. Le SAE peut comporter plusieurs règles de conservation/destruction ; chaque série, dossier, sous-dossier et volume est lié à une ou plusieurs règles ; elles peuvent aussi s'appliquer aux documents ; une règle de conservation/destruction peut viser un type de document.

## Document à archiver/archivé

Au cœur du système se trouve l'entité la plus importante de toutes : les documents archivés. Ils constituent le fondement de l'infrastructure d'archivage, dans la mesure où ils tracent les activités de l'entreprise/organisation.

Les documents archivés sont constitués d'une ou plusieurs pièces ; une même pièce peut apparaître dans plusieurs documents.

Les documents sont normalement classés dans des volumes. Ils peuvent aussi être archivés dans une série (exception déjà évoquée). MoReq2 autorise une configuration qui empêche l'usage de volumes et/ou de sous-dossiers, en ne laissant que les sous-dossiers ou les dossiers. Un document ne peut être classé que dans un volume, un sous-dossier, un dossier ou une série.

## Type de document archivé

Les documents archivés sont rattachés à un type de document, dans le but de faciliter la gestion dans le SAE. Exemples de type de document : facture, page web, etc.

## Composant

Chaque document ou chaque pièce est constitué d'au moins un composant et parfois de plusieurs. Ainsi une simple page web peut n'avoir qu'un composant - un fichier HTML - tandis qu'une page plus complexe sera composée de douzaines de fichiers : HTML, GIF, JPEG, etc.

## 13.4 MODELE DE CONTROLE D'ACCES

---

Cette section comporte un modèle assez simple pour illustrer les profils dans un SAE.

La matrice identifie deux profils principaux, eux-mêmes subdivisés en d'autres profils. Les premiers sont les utilisateurs et les administrateurs, avec des droits d'accès différents dans le SAE.

Le nombre des profils figurant dans le modèle n'est qu'indicatif. Cela ne signifie pas que les entreprises/organisations devraient créer ces profils-là, ni même ce nombre-là de profils. Chaque structure définira les profils dont elle a besoin, et leur nombre variera sans doute dans le temps.

Les profils ci-après donne un exemple des droits de contrôle d'accès pour certaines fonctionnalités, en fonction des responsabilités.

Il y a quatre profils dans la matrice proposée :

- Administrateur central - ce profil contrôle la configuration de tout le SAE et la gestion des documents archivés.
- Administrateur local - ce profil a des droits sur un sous-ensemble du SAE ou du plan de classement. Ces profils sont utiles en cas d'éclatement géographique de l'organisation.
- Réviseur - c'est un profil particulier lié à la mise en œuvre du sort final défini par les règles de conservation/destruction.
- Utilisateur final - l'utilisateur final correspond au niveau d'accès standard ; il s'agit de ceux qui doivent archiver des documents dans le SAE ou qui ont besoin d'y rechercher des documents pour leur travail quotidien.

Cette séparation en deux profils des administrateurs n'est qu'un exemple ; les responsabilités peuvent être réparties autrement. Dans de petites structures, cette division paraîtra inutilement complexe car une seule personne peut contrôler toute l'administration. Dans de grandes organisations ce sera insuffisant au contraire et il faudra sans doute plus de deux profils (records manager, responsable administratif, archiviste, gestionnaire de données, responsable informatique). MoReq2 ne préjuge pas du nombre d'administrateurs nécessaire à telle ou telle organisation.

Le profil d'un administrateur local est ici un exemple. Ce profil peut avoir plusieurs intitulés selon les organisations : ce pourra être responsable administratif local, ou utilisateur privilégié, etc.

En tout état de cause et d'un point de vue système, les administrateurs ne font que mettre en œuvre les décisions de la direction générale. Et ces décisions sont basées sur les besoins métier et la politique d'archivage. Ces décisions se fondent aussi sur l'environnement réglementaire : lois sur l'information, la sécurité des données, les archives et les règles industrielles (voir à ce sujet le point 11.5).

Cette matrice ne sous-entend pas que les administrateurs doivent prendre des décisions de fond bien que cela puisse arriver.

Le profil des administrateurs porte sur l'organisation de l'archivage ; ils ont vocation à gérer les documents à archiver et archivés en tant que tels et non leur contenu ou le contexte métier. Ils sont aussi responsables des aspects matériel et logiciel du SAE et du stockage ; ils contrôlent l'exécution des sauvegardes et la performance du SAE.

De nombreuses entreprises/organisations ont besoin d'intégrer la gestion des processus métier avec l'archivage. Il y a lieu alors de créer une série spécifique d'autorisations pour les gestionnaires métier,

incluant éventuellement la faculté de contrôler et de gérer un groupe particulier d'utilisateurs ou une branche du plan de classement.

MoReq2 parle de l'utilisateur mais il y a, dans la plupart des cas, des profils différents d'utilisateur et le SAE ne devrait pas limiter le nombre de ces profils au moment de la configuration.

Si on prend l'exemple d'un gestionnaire de dossiers sériels (voir le point 10.5 - Dossiers sériels), il aura des autorisations spécifiques au sein d'une branche du plan de classement.

A l'inverse des administrateurs, les utilisateurs ont accès aux fonctionnalités dont un collaborateur a normalement besoin, notamment l'archivage de nouveaux documents et la recherche et le repérage de documents archivés. Ils s'occupent des contenus, des caractéristiques ou du contexte des documents, et non de leur gestion car ils sont surtout concernés par les processus métier tracés dans les documents.

Dans la matrice, le profil d'utilisateur final montre des droits d'accès qui conviennent à la majorité des utilisateurs pour mener à bien leurs tâches courantes.

Autre exemple de profil : le réviseur. Il s'agit d'un niveau de contrôle d'accès qui peut être attribué à un sous ensemble des utilisateurs dans le but de passer en revue les documents archivés.

Cette matrice doit être vue comme un point de départ, une base pour l'attribution des droits. Les utilisateurs de ces spécifications devront prendre en considération d'autres exigences liées à leur environnement spécifique.

Les exigences liées à ce tableau figurent à la section 4.1 ; elles insistent sur le fait que l'exigence n'est pas pour le SAE d'inclure la matrice d'accès-type présentée ici mais bien d'être capable de configurer les différents niveaux d'accès d'une matrice définie par l'entreprise/organisation, avec un nombre et une typologie de profils et de fonctions non limités. Il doit être possible de compléter chaque case de la matrice avec « oui » ou « non », dans un tableau comportant autant de colonnes que nécessaire.

D'autres profils peuvent être identifiés et mis en œuvre, par exemple :

- assistant ;
- auditeur ;
- correspondant CNIL ;
- décideur ;
- producteur ;
- records manager;
- superviseur.

Cette matrice est divisée en rubriques qui regroupent, par commodité, des tâches habituellement associées aux séries et aux dossiers, aux documents, à l'archivage et à l'administration.

Tâches	Profils			
	Utilisateurs		Administrateurs	
	Utilisateur final	Réviseur	Administrateur Local	Administrateur Central
Ajouter de nouvelles séries	Non	Non	Oui	Oui
Créer de nouveaux dossiers	Oui	Non	Oui	Oui
Modifier les métadonnées d'un dossier	Non	Oui	Oui	Oui
Maintenir le plan de classement et les dossiers	Non	Non	Oui	Oui
Détruire des dossiers	Non	Non	Oui	Oui
Capturer les documents	Oui	Non	Oui	Oui
Reclasser un document dans un autre dossier	Oui	Non	Oui	Oui
Rechercher et consulter un document archivé	Oui	Oui	Oui	Oui
Modifier le contenu des documents archivés	Non	Non	Non	Non
Modifier les métadonnées de documents archivés	Non	Oui	Oui	Oui
Détruire des documents archivés	Non	Non	Oui	Oui
Décider ou suspendre un gel	Non	Oui	Oui	Oui
Gérer les règles de conservation/destruction et le sort final	Non	Oui	Oui	Oui
Exporter et importer des dossiers et des documents	Non	Oui	Oui	Oui
Consulter les historiques	Non	Oui	Oui	Oui
Configurer et gérer l'historique	Non	Non	Non	Oui
Modifier les données d'historique	Non	Non	Non	Non
Transférer les données d'historique sur un support hors ligne	Non	Non	Oui	Oui
Exécuter toutes les opérations relatives aux utilisateurs et à leurs droits d'accès	Non	Non	Oui	Oui
Attribuer des autorisations d'accès aux administrateurs locaux	Non	Non	Non	Oui
Déléguer ses autorisations d'accès à d'autres utilisateurs	Oui	Oui	Oui	Oui
Créer et gérer des profils de gestionnaires de dossiers	Non	Non	Non	Oui
Maintenir les bases de données et le stockage	Non	Non	Oui	Oui
Maintenir les autres paramètres du système	Non	Non	Non	Oui
Définir et consulter les autres rapports du système	Non	Oui	Oui	Oui