Concepts

Sommaire

Introduction

Maarch RM est le tout nouveau produit issu des laboratoires Maarch. Basé sur un framework puissant spécialisé dans la gestion documentaire d'entreprise (Laabs), il suit à la lettre les dernières normes en termes d'archivage à valeur probatoire.

Au niveau opérationnel, Maarch RM permet à minima de :

- Réguler les versements dans le SAE au travers de conventions portant sur la provenance, la fréquence, et les formats des archives et de leur metadonnées
- Conserver de grandes quantités de ressources électroniques (documents, courriels, vidéos, archives, etc.) avec toutes les garanties d'intégrité et de pérennité
- Communiquer rapidement ces ressources au travers d'interfaces natives ou d'applications métier
- Disposer de pistes d'audit fiables et opposables sur l'ensemble des archives et des journaux de production
- Gérer le cycle de vie des archives (déplacement, tri, destruction, restitution)

D'autres fonctions non spécifiques au SAE sont également présentes :

- Organiser la circulation des documents au travers d'étapes d'indexation/validation
- Effectuer des versements transactionnels ou en sortie de numérisation

Enfin, Maarch RM dispose d'une grande souplesse et d'un framework idéal pour répondre à n'importe quel besoin métier à vocation documentaire.

Ce document décrit de manière synthétique les fonctionnalités du logiciel en termes de :

- Versement
- Conservation/stockage
- Cycle de vie
- Communication
- Restitution

Versement des archives

« Le versement est l'opération par laquelle le service versant transmet un document au service d'archive pour sa conservation. En retour, le service d'archive délivre une attestation de dépôt qui contient toutes les informations relatives à l'opération et qui certifie que le système répond bien aux exigences définies dans la convention d'archivage pour le niveau de service requis. »

Le versement peut être réalisé par un utilisateur de l'application au travers des écrans de manière interactive ou bien par un traitement en arrière-plan afin de procéder au versement d'un ensemble d'archives.

La définition des acteurs, des fonctions et des entités du modèle est fournie dans les documents de spécifications de l'application. Le **DDTS** (Dossier de Descriptions Techniques du Système) fournit l'ensemble des informations sur l'architecture logique et physique, le modèle de données utilisé et les procédures techniques associées.

Versement par lot

Il s'agit de verser dans le SAE des lots d'archive homogènes possédant les mêmes caractéristiques et qui seront soumises aux mêmes règles de gestion.

Les ressources numériques à archiver sont mises à disposition dans un répertoire, chacun accompagné d'un fichier fournissant les métadonnées descriptives associées. Les métadonnées de gestion des nouvelles archives sont déterminées en utilisant les référentiels du système d'archivage: profil, convention et niveau de service.

Format de métadonnées compatible Maarch v1

Les métadonnées sont fournies sous la forme d'un fichier XML portant le même nom que le document numérique à archiver. Le fichier doit posséder une extension ".xml". Les données sont structurées conformément au modèle de métadonnées descriptives de l'implémentation.

Exemple de contenu de métadonnées au format XML :

```
<?xml version="1.0" encoding="UTF8" ?>
 <invoice>
     <date>2009-07-15</date>
     <reference>F2009-295</reference>
     <purchaseOrderReference>PO2009-095</purchaseOrderReference>
     <thirdPartyName>FORTIS</thirdPartyName>
     <thirdPartyContact>John MURPHY</thirdPartyContact>
     <currency>EUR</currency>
     <totalAmount>29250</totalAmount>
     <documentType>accountsPayable</documentType>
     <taxAmount>5850</taxAmount>
     <companyName>MAARCH</companyName>
     <accountingPeriod>2009</accountingPeriod>
 </invoice>
```

Bordereaux de métadonnées SEDA / MEDONA

SEDA et MEDONA sont des modèles standards pour les transactions d'échange entre les acteurs du SAE.

Le SEDA est le "Standard d'Echange de Données pour l'Archivage" relatif aux données d'archives publiques. Il a été créé en 2006 par la Direction des Archives de France et la Direction Générale pour la Modernisation de L?État, et révisé en 2010 (v0.2), en 2012 (v1.0) et plus récemment en 2015 (v2) pour assurer sa compatibilité avec la norme MEDONA. Il comporte à la fois le modèle fonctionnel et un modèle de données pour les échanges de données d'archive de la sphère publique : description, acteurs, règles de gestion, référentiels métier et techniques.

La norme AFNOR NF Z44-022, intitulée "Modèle d'Echange de DONnées pour l'Archivage" ou MEDONA a été publiée en 2014. Elle est basée sur le SEDA, dont elle reprend le modèle fonctionnel, elle s'ouvre à tous les standards de description des archives et à tous les référentiels. Un bordereau MEDONA est composé :

- d'un en-tête
- d'une déclaration des objets binaires
- d'une description de ces objets
- des déclarations du service versant et du service d'Archives

L'en-tête indique l'identifiant du lot et celui de la convention de versement :

```
<?xml version="1.0"?>
<ArchiveTransfer xmlns="org:afnor:medona:1.0">
   <Date>2015-06-22T07:47:32</Date>
   <MessageIdentifier>ArchiveTransfer_invoices_300</MessageIdentifier>
   <ArchivalAgreement>MAARCH_WA_invoice</ArchivalAgreement>
   <CodeListVersions/>
```

Vient ensuite la déclaration des objets binaires (DataObjectPackage > BinaryDataObject) : les fichiers PDF des factures :

```
<DataObjectPackage>
    <BinaryDataObject xml:id="bdo_003">
        <Attachment filename="F_10.pdf"/>
        <Format>application/pdf</Format>
        <MessageDigest algorithm="md5">135a4450230383f6ec190b8b3f366755</MessageDigest>
        <SignatureStatus>valide</SignatureStatus>
        <Size>97538</Size>
    </BinaryDataObject>
```

Puis dans la partie Metadata on trouve les index :

```
<DescriptiveMetadata>
      <archivePackage xmlns="maarch.org:laabs:medona">
          <archive xmlns="maarch.org:laabs:recordsManagement">
              <descriptionObject>
                  <adminDescription xmlns="maarch.org:laabs:businessRecords">
                      <date>2007-02-12</date>
                      <reference>F2007-011</reference>
                      <thirdPartyName>STERIA</thirdPartyName>
                      <companyName>MAARCH</companyName>
                      <year>2007</year>
                      <companyCode>MAARCH</companyCode>
                  </adminDescription>
              </descriptionObject>
              <document xmlns="maarch.org:laabs:documentManagement" oid="bdo_003"/>
          </archive>
```

En fin de message figurent les identités du service d'Archives et du service versant :

```
<ArchivalAgency>
        <Identifier>123456789_Archives</Identifier>
        <OrganizationDescriptiveMetadata>
            <organization xmlns="maarch.org:laabs:organization">
                <orgName>ACME</orgName>
            </organization>
        </OrganizationDescriptiveMetadata>
    </ArchivalAgency>
    <TransferringAgency>
        <Identifier>45239273100025_Finance</Identifier>
        <OrganizationDescriptiveMetadata>
            <organization xmlns="maarch.org:laabs:organization">
                <orgName>Maarch SAS</orgName>
            </organization>
        </OrganizationDescriptiveMetadata>
    </TransferringAgency>
 </ArchiveTransfer>
```

Maarch enchaîne de façon automatique ou manuelle les 3 grandes étapes du processus de versement :

1. Transfert : envoi dans le sas d'un bordereau ? contrôles
2. Validation : acceptation du transfert par l'archiviste
3. Traitement : constitution des paquets d'archive et écriture en Y

Versement interactif

Maarch permet aussi le versement via l'interface d'un bordereau SEDA ou MEDONA, avec ou sans pièce incorporée.

Profils d'archivage

Le profil d'archivage regroupe un ensemble de règles prédéfinies applicable aux dépôts d'archive, en termes de confidentialité, de conservation et de constitution des métadonnées. Il évite de préciser ces règles pour chaque archive versée dans le système d'archivage, ce qui pourrait s'avérer long et fastidieux. Chaque archive peut donc faire référence à un et un seul profil. Il est aussi possible de modifier les archives afin de préciser des règles spécifiques qui annulent et remplacent, partiellement ou totalement, celles du profil auquel elles font référence.

Les profils d'archivage sont administrés par les personnes habilitées dans le système d'archivage via l'interface graphique utilisateur.

Format de métadonnées descriptives

La gestion des métadonnées descriptives est liée à l'implémentation dans le système d'archivage d'un ensemble de composants répondant à des règles techniques strictes. Ces règles sont définies dans le DDTS.

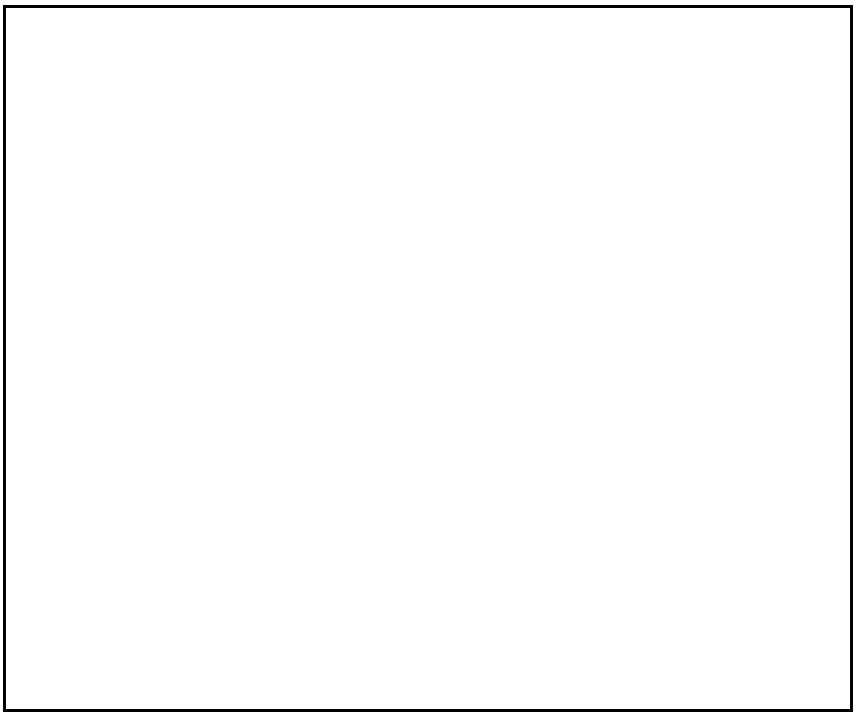
Dans le cas où les métadonnées descriptives sont conservées au **format balisé XML**, le profil permet de préciser un nom de schéma à appliquer pour le contrôle des métadonnées lors du versement.

Deux formats de schéma sont pris en charge:

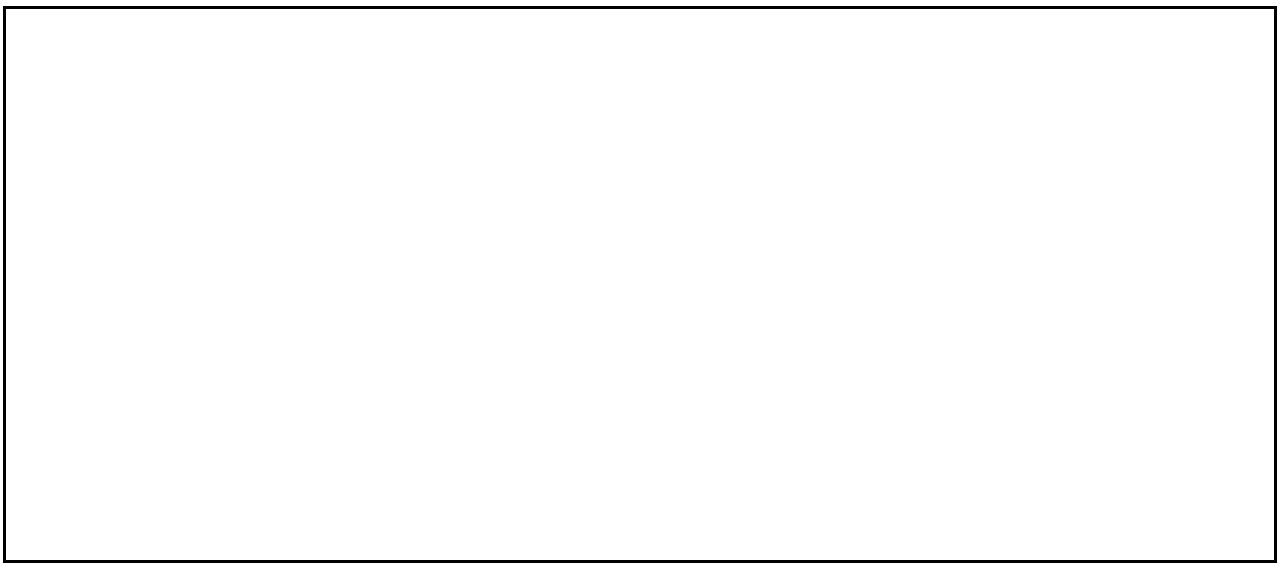
- xsd (XML Schema Definition)
- rng (RelaxNG)

L'application Maarch RM fournit les outils techniques de validation des données XML par ces deux types de schémas. C'est typiquement la méthode utilisée pour enregistrer des schémas descriptifs imbriqués de type SEDA (Système d'Echange de Documents d'Archive)

Dans le cas où les métadonnées descriptives sont conservées dans une **base de données** relationnelle, la classe de description fournit un jeu de métadonnées disponibles en base de données pour le profil d'archivage. On peut ensuite sélectionner quelles données seront utilisées par les archives et lesquelles seront obligatoires.



Règles du profil



Les règles du profil permettent de déterminer :

- la date de référence pour le calcul du délai de conservation
- la durée de conservation théorique
- le sort final

Le code d'accès est une référence qui permet de lier le profil et toutes les archives qui l'utilisent au référentiel de sécurité des archives.

Chaque code liste les groupes d'utilisateurs habilités pour les différentes opérations sur les archives ou les profils.

Certificat de dépôt

Conformément aux normes, Maarch RM produit des attestations pour chaque événement du cycle de vie des archives (dépôt, communication (conformité), modification (règle de conservation, gel/dégel du cycle de vie)).

Afin de produire l'attestation, le système valide la possibilité d'attribuer l'événement à une ou deux parties intervenant : à minima le service d'archive responsable de la conservation et pour certaines attestations le tiers à l'origine de l'opération (service versant, service producteur notamment).

Lors du dépôt d'archives par lot, le service versant et le service d'archive sont identifiés grâce à la convention d'archivage utilisée, dont la référence doit obligatoirement être précisée par l'opérateur et dont la validité est vérifiée par le système.

Les attestations sont produites selon le cas dans deux ou trois formats de sortie:

1. Une copie dans le journal du cycle de vie de l'archive, qui permet d'exploiter les attestations au travers des écrans de recherche et de consultation du journal du cycle de vie
2. Une copie sous forme de document XML dans un répertoire de sortie, qui permet au service d'archive de collecter et transmettre les attestations par lot aux services concernés
3. Le cas échéant, une copie à l'écran pour affichage et impression par le demandeur

La procédure de versement par lot produit une attestation de dépôt lorsque toutes les étapes du versement ont été effectuées et validées :

- Validation des métadonnées de gestion
- Validation des métadonnées descriptives
- Attribution d'un identifiant unique
- Calcul de l'empreinte
- Vérification du format du document
- Écriture des métadonnées descriptives et de gestion
- Stockage redondant du document numérique

La procédure transmet au composant responsable de la production de l'attestation l'archive nouvellement versée et le chemin répertoire choisi par l'opérateur vers lequel produire le document d'attestation correspondant au format XML.

```
<?xml version="1.0"?>
 <certificateOfDeposit>
     <archiveId>gQPm3ao2q9iZ</archiveId>
     <timestamp>2015-02-05T09:29:42.301316Z</timestamp>
     <hash algorithm="SHA256">0038958cfdd3bf9f56fdf32524bf60a45edd9728d?</hash>
     <address>/var/repository/archives_1/DRM/2015/02/05/00000001/0057</address>
     <archiverOrg>
             <displayName>Maarch</displayName>
             <legalClassification/>
             <taxIdentifier/>
             <registrationNumber/>
     </archiverOrg>
     <depositorOrg>
             <displayName>ACME</displayName>
             <legalClassification/>
             <taxIdentifier/>
             <registrationNumber/>
     </depositorOrg>
 </certificateOfDeposit>
```

Ceci fait, l'attestation existe en deux exemplaires: l'un dans le journal du cycle de vie de l'archive, l'autre dans un répertoire pour transmission au service versant.

Contrôle et validation des entrées

Contrôle du format

Maarch RM met en ?uvre un contrôle du format des documents numériques afin de les associer à un format connu, et de valider leur conformité aux exigences normatives et contractuelles.

Maarch RM s'appuie sur le référentiel des formats PRONOM développé et maintenu par le département *Digital Preservation* des Archives Nationales du Royaume-Uni.

Site officiel: http://apps.nationalarchives.gov.uk/PRONOM

Le tableau ci-dessous décrit les informations contenues dans le référentiel pour chaque format:

Information	Description
ID	Identifiant unique du format dans le référentiel
PUID	Identifiant unique PRONOM utilisé comme référence pour les documents numériques archivés par Maarch RM
Nom	Nom du format
Version	Version du format (facultatif)
Type MIME	Multipurpose Internet Mail Extension, identifiant de format largement utilisé dans les technologies internet (facultatif)
Extension	Extensions possibles pour les fichiers utilisant le format (facultatif)
Signature interne	Identifiant des signatures internes au format de fichier qui permettent sa détermination par une analyse du contenu
Priorité sur format	Identifiant des formats sur lesquels le format aura la priorité lors de la détermination du format de contenu (facultatif)

Le référentiel des formats PRONOM est livré sous la forme d'un fichier XML dans la dépendance de gestion du système de fichiers, accompagné d'un outil de détermination des formats qui utilise le système de signature interne.

Le référentiel est périodiquement augmenté et mis à jour par des contributions ou le département *Digital Preservation* des Archives Nationales du Royaume-Uni. Il est librement téléchargeable sur le site officiel et peut ainsi être mis à jour dans l'application.

Maarch RM est un système ouvert qui permet d'implémenter les règles de la norme. La liste des formats de fichiers n'est pas imposée par le logiciel, mais l'application stricte des règles de la norme impose de restreindre la liste des formats à ceux qui permettent la pérennisation de l'information et la restitution fidèle dans le temps des documents archivés.

A ce titre, les formats de documents numériques acceptés par défaut dans la configuration sont les suivants:

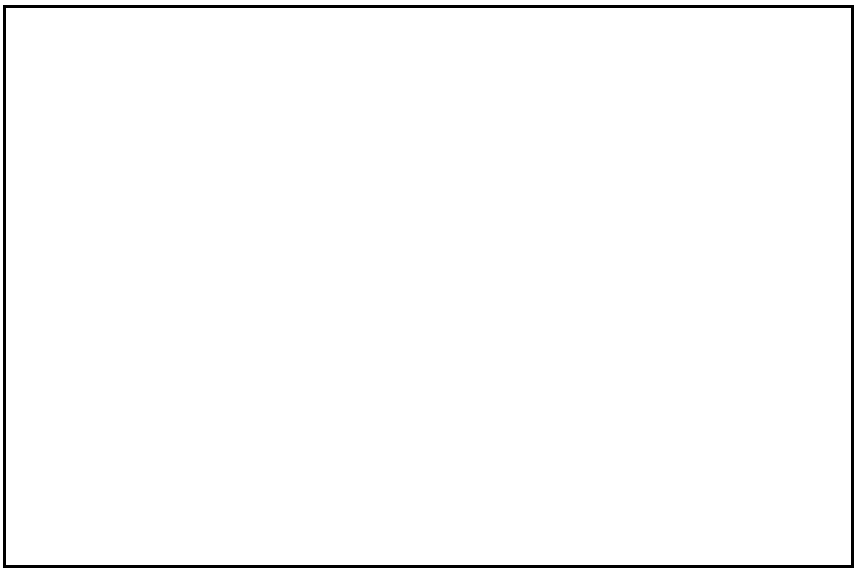
- Adobe Acrobat PDF 1.4 et supérieurs (1.4, 1.5, 1.6, 1.7)
- Adobe Acrobat PDF/A (1.a, 1.b, 2.A, 2.b, 2.u, 3.A, 3.b, 3.u)

Il existe trois cas dans lesquels le document numérique peut être rejeté à cause de son format:

- Le format n'a pas pu être déterminé
- Le format est déterminé mais n'est pas conforme ou valide du point de vue de sa norme
- Le format n'est pas autorisé comme format d'archivage numérique

Dans ces trois cas, le document ne peut être versé dans l'archive étant donné qu'aucune procédure de conversion de format n'est prévue dans la version actuelle de l'application.

Les formats autorisés sont gérés au sein de la convention existant entre un service versant et un service d'archive :



Identifiant unique d'archive

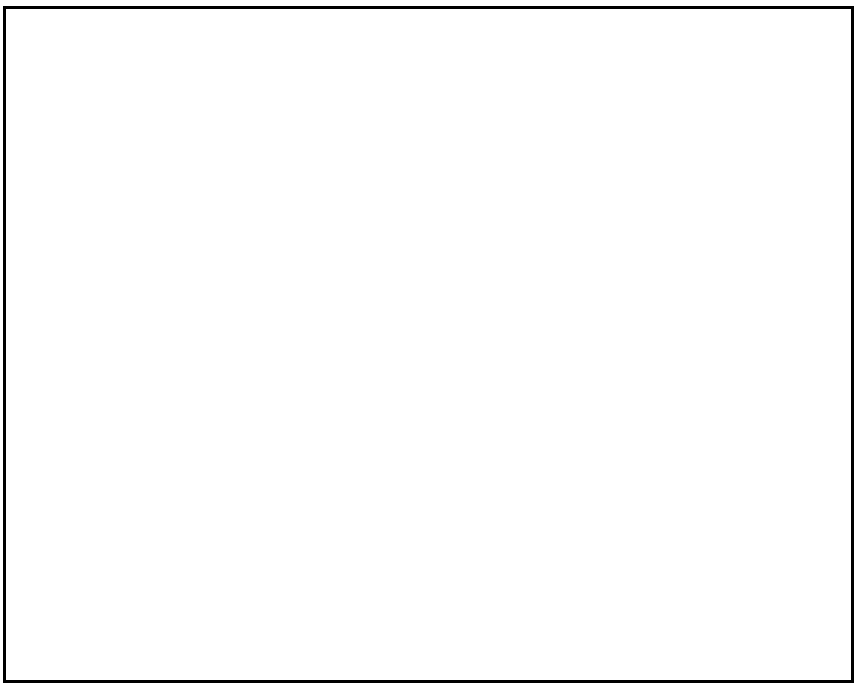
Maarch RM gère un identifiant unique pour les archives versées dans le système. Cet identifiant est attribué automatiquement par le système selon l'algorithme "Mersenne Twister" associé à l'horloge du serveur.

Il en résulte un identifiant unique sur le système constitué de 16 caractères au maximum.

Un préfixe représentant l'identifiant unique de l'instance du système d'archivage, par exemple le nom du domaine internet de l'hébergement, peut être ajouté afin de rendre l'identifiant universel.

L'unicité de l'identifiant d'archive est contrôlée dans le système de sorte qu'il est impossible à deux archives de posséder un même identifiant. De plus, le système autorise de préfixer les identifiants qu'il attribue (par exemple le nom du domaine internet de l'hébergement) afin d'assurer l'universalité de l'unicité de l'identifiant.

L'identifiant d'archive est utilisé pour les métadonnées de gestion, les métadonnées descriptives, et pour la ressource numérique.



Stockage et gestion des archives

Prise en compte des métadonnées

La procédure d'enregistrement prévoit la prise en charge de métadonnées descriptives dans un format d'échange standardisé.

L?identité de l?organisme qui procède au transfert des documents à archiver et celle du service d'archive sont issues de la convention d'archivage obligatoirement précisée lors du versement.

La date et l'heure de création ou d'arrivée de l'archive dans le système est déterminée par l'horodatage du transfert.

Les formats de contenu et d'encodage sont identifiés et validés par des outils de détermination et de contrôle des formats. Le document numérique est référencé avec un identifiant de format du référentiel PRONOM.

La durée de conservation et le sort final des documents à archiver sont issus du profil d'archivage obligatoirement précisé lors du transfert.

Les droits d'accès sont basés sur un code d'accès dont découlent les règles de contrôle d'accès; ce code est lui aussi issu du profil d'archivage.

Horodatage

Par défaut, Maarch RM utilise la date du système hôte de l'application pour l'horodatage des événements, avec une précision d'une microseconde. Le système doit donc assurer la synchronisation de son horloge avec un service d'horodatage fiable.

En mode projet, il est aussi possible de faire appel à un service externe d'horodatage, généralement payant.

Le format de représentation des horodatages est conforme à la norme ISO 8601 et comporte la date, l'heure avec la précision d'une microseconde et le fuseau horaire.

Exemple: 2015-01-01T14:56:33,836352Z

Copies de sécurité

Maarch RM permet de déclarer les supports de stockage des documents numériques et de les regrouper dans des grappes de stockage. Une grappe de stockage permet de définir que plusieurs sites de stockage possèdent une même priorité en écriture, ce qui provoque une écriture redondante des documents au moment du dépôt.

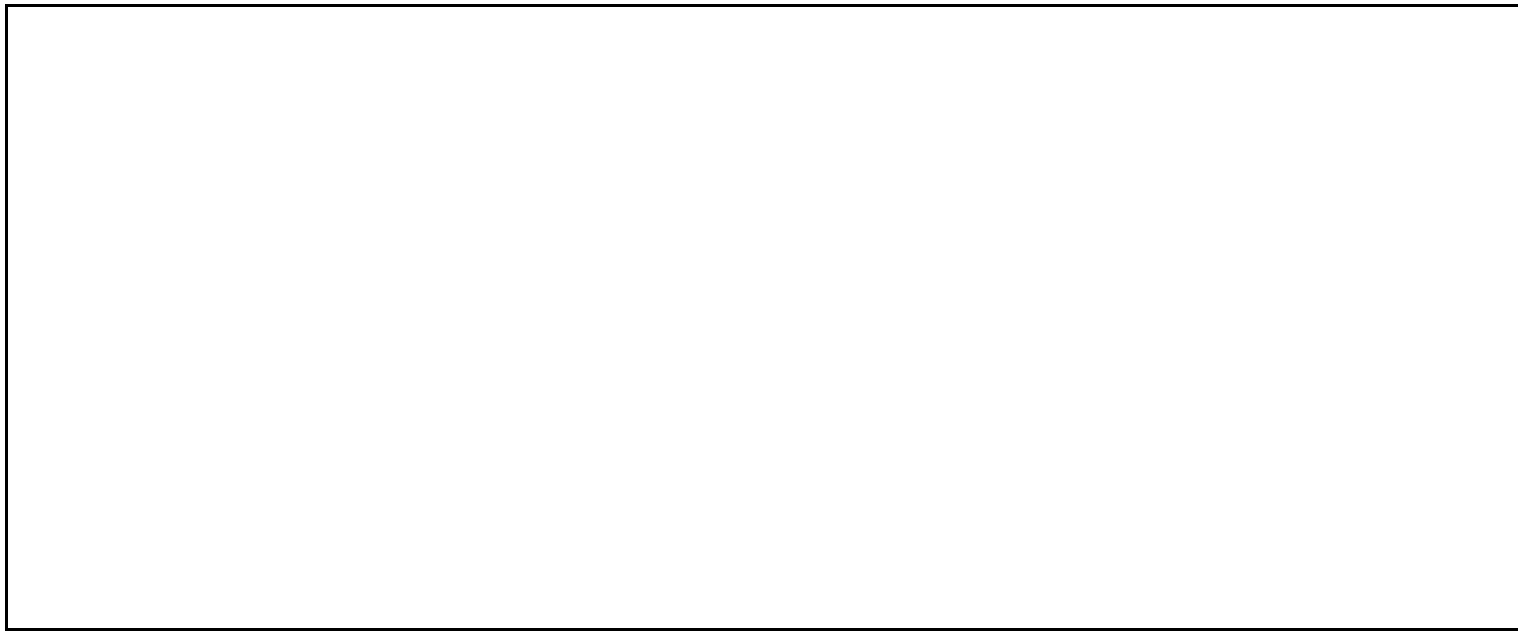
Le niveau de service utilisé lors du versement par lot possède un indicateur de redondance, qui activé provoque le contrôle par la procédure que la grappe de stockage utilisée possède bien au moins deux sites de dépôt avec la même priorité la plus basse. Si ces conditions ne sont pas remplies, la procédure de versement lève une erreur et n'autorise pas le dépôt.

Lors de l'écriture, le système procède de la sorte sur chaque site :

- Calcul de l'empreinte numérique du document avant écriture
- Attribution d'un nom de fichier (chemin répertoire et nom de fichier) unique sur le site
- Écriture du fichier
- Lecture du fichier et validation que l'empreinte du fichier écrit correspond à celle du fichier reçu

Les deux sites étant gérés au sein d'un même cluster (grappe) de dépôt, l'adresse de stockage d'un document est identique pour les deux supports.

Les grappes de dépôt sont gérées dans l'interface d'administration du système :



Calcul d'empreinte

L'application Maarch RM utilise des supports de stockage réinscriptibles. La norme exige dans ce cas le calcul d'une empreinte au moment du dépôt selon un algorithme choisi lors de la configuration.

L'empreinte est ensuite vérifiée à plusieurs étapes du cycle de vie:

- Lors de la communication / attestation de conformité
- Lors de la restitution
- Par un contrôle périodique de l'archive

Une cinquantaine d'algorithmes de calcul d'empreinte sont activables.

Destruction

Maarch RM implémente un algorithme d'effacement sécurisé pour la destruction des documents archivés sur support réinscriptible, nommé **DoD 5220.22-M**.

Il est utilisé pour la suppression des documents numériques des supports de stockages lors des opérations de destruction d'archive, mais aussi de retour arrière en cas d'erreur lors du dépôt ayant lieu après l'écriture du document. En effet, le dépôt consiste en une triple écriture : au moins une double écriture sur deux supports pour le document numérique, plus l'écriture des métadonnées de gestion et descriptives. Dans le cas où la seconde écriture du document ou l'écriture des métadonnées serait un échec, il faut donc effacer de manière sécurisée la première écriture du document

numérique.

L'effacement met en ?uvre les actions suivantes :

Passe 1 : L'application génère un octet (8 bits) aléatoire qu'elle écrit dans tous les secteurs du fichier à effacer.

Passe 2 : L'application calcule l'octet complémentaire à l'écriture de la 1ère passe qu'elle écrit dans tous les secteurs du fichier à effacer.

Passe 3 : L'application génère un nouvel octet aléatoire ? obligatoirement différent du précédent complément ? qu'elle écrit dans tous les secteurs du fichier à effacer.

Passe 4 : Suppression logique du fichier par le système d'exploitation (unlink/del)

Production d'attestations

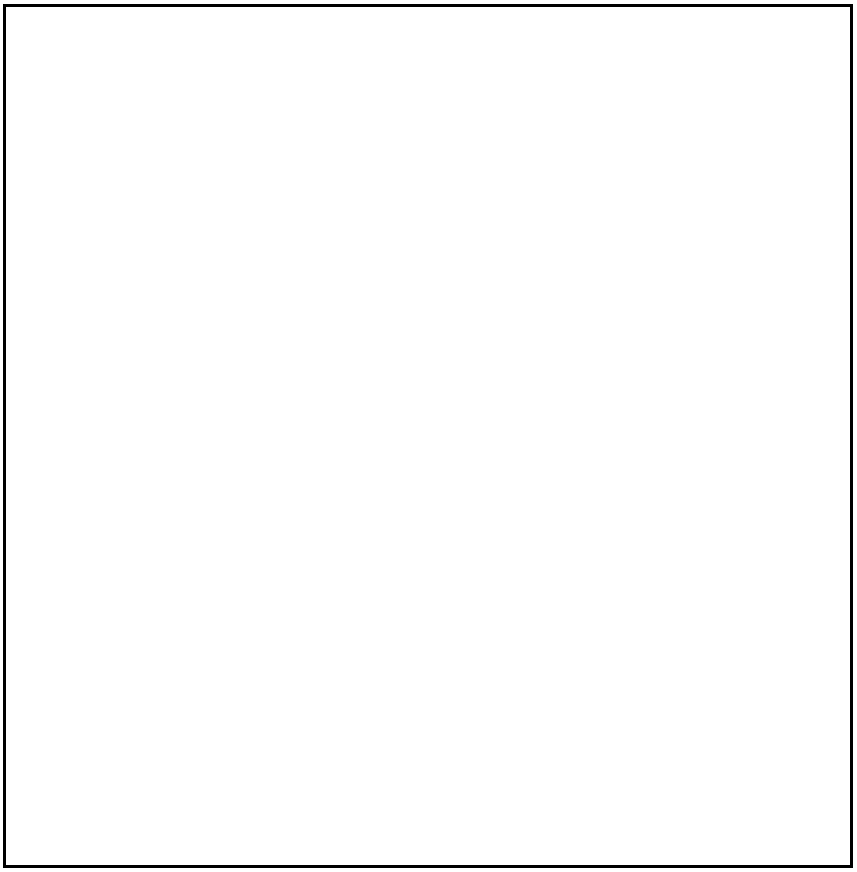
Hormis le certificat de dépôt vu plus haut, Maarch RM produit des attestations visant à garantir la conformité des opérations du SAE.

Attestation de conformité

La production de l'attestation de conformité est exigée par la norme. Elle a pour objectif de valider l'intégrité et la fidélité de l'archive communiquée au lecteur. Cette attestation est produite après vérification de l'archive communiquée.

La demande est faite par une personne habilitée, c'est-à-dire

- qui possède les privilèges nécessaires pour demander une attestation de conformité
- qui possède les droits d'accès pour accéder aux informations de l'archive
- qui possède les droits d'accès pour communiquer l'archive
- qui est positionnée dans une organisation partie prenante dans le système d'archivage



L'attestation produite est affichée à l'écran et l'utilisateur peut l'imprimer. Une copie est enregistrée dans le journal du cycle de vie de l'archive.

Attestation de modification

Elle est produite lorsqu'un opérateur habilité modifie les informations de conservation de l'archive:

- la date de début de calcul
- la durée
- le sort final
- gel de l'application de la règle
- dégel de l'application de la règle

La demande est faite par une personne habilitée, c'est-à-dire

- qui possède les privilèges nécessaires pour modifier une archive
- qui possède les droits d'accès pour accéder aux informations de l'archive à modifier
- qui possède les droits d'accès pour modifier l'archive
- qui est positionnée dans une organisation partie prenante dans le système d'archivage

L'attestation produite est enregistrée dans le journal du cycle de vie de l'archive, une copie dans le répertoire de sortie au format XML.

Attestation de restitution

La procédure d'élimination par lot produit une attestation de restitution s'il s'agit du sort final du document, lorsque toutes les étapes de la restitution ont été effectuées et validées:

- Récupération des métadonnées
- Récupération du document
- Contrôle d'empreinte du document
- Écriture des métadonnées descriptives et de gestion dans la sortie
- Écriture du document numérique dans la sortie

La procédure transmet au composant responsable de la production de l'attestation l'archive restituée et le chemin répertoire choisi par l'opérateur vers lequel produire le document d'attestation correspondant au format XML.

Ceci fait, l'attestation existe en deux exemplaires: l'un dans le journal du cycle de vie de l'archive, l'autre dans un répertoire pour transmission au service versant.

Attestation sur profil d'archivage

Elle est produite lorsqu'un opérateur habilité ajoute, modifie les informations ou supprime un profil d'archivage.

La demande est faite par une personne habilitée, c'est-à-dire

- qui possède les privilèges nécessaires pour gérer les profils d'archivage
- qui possède les droits d'accès pour accéder aux informations du profil à gérer le cas échéant
- qui possède les droits d'accès pour modifier le profil le cas échéant
- qui est positionnée dans une organisation partie prenante dans le système d'archivage

L'utilisateur accès à la liste des profils par l'écran d'administration. Il effectue les opérations souhaitées, ajoute un profil et/ou saisit de nouvelles informations sur un profil ou supprime un profil.

L'attestation produite est enregistrée dans le journal du cycle de vie de l'archive, une copie dans le répertoire de sortie au format XML.

Sécurité

Authentification de l'utilisateur

Le logiciel Maarch RM utilise un contrôle d'accès par couple utilisateur et mot de passe.

Toute connexion au logiciel est historisée dans le journal d'audit de l'application avec le nom de l'utilisateur ainsi que la date et heure de connexion.

Les tentatives de connexion infructueuses sont aussi historisées.

Il est possible de définir une politique de sécurité des authentifications d'utilisateur selon plusieurs règles:

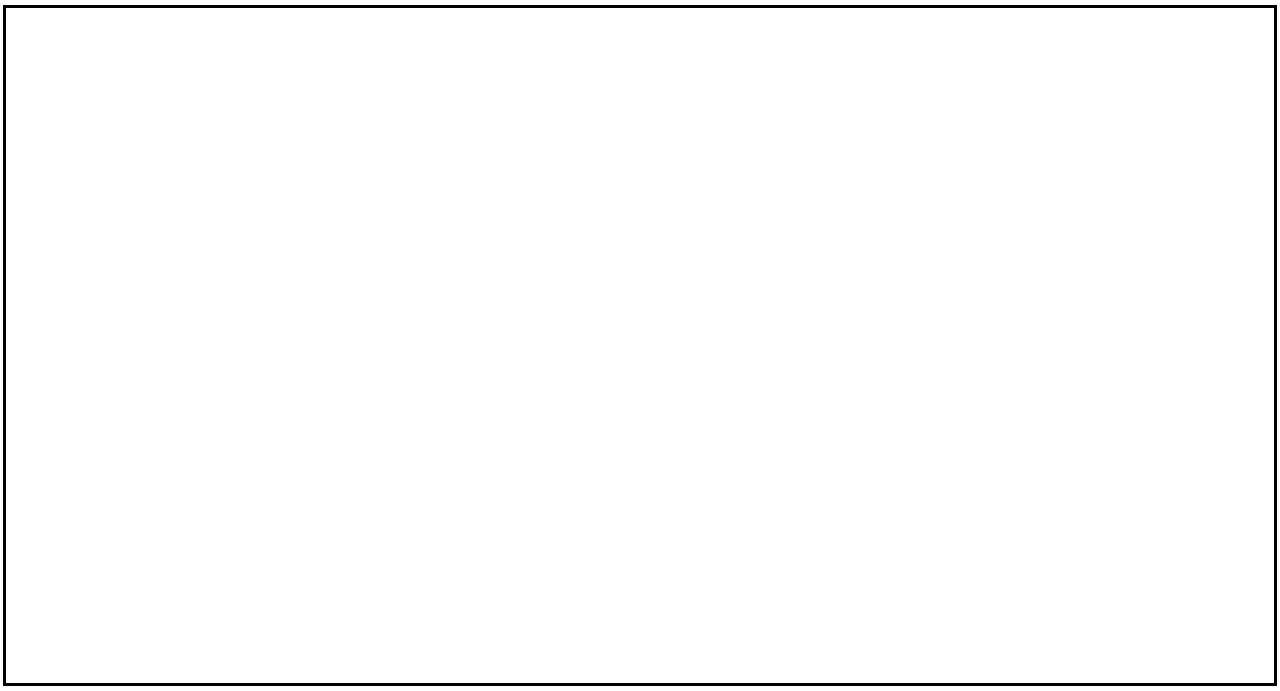
- Le nombre de tentatives de connexion infructueuses au-delà duquel le compte d'utilisateur est verrouillé.
- La durée de validité du mot de passe pour forcer le changement de mot de passe des utilisateurs de manière périodique
- La complexité du mot de passe: longueur minimale, présence de chiffres, de caractères mixtes, de caractères spéciaux.

Autorisations

L'utilisateur connecté est positionné dans un ou plusieurs groupes d'autorisation qui définissent les droits des utilisateurs selon deux axes: l'accès aux fonctions et l'accès aux données.

L'accès aux fonctions est assuré par un système de privilèges qui liste pour un groupe tous les services de l'application auxquels il a droit.

L'accès aux données permet de définir pour le groupe la liste des entités du modèle de données auxquelles il peut accéder en précisant le nom de la classe des entités (type d'objet) ainsi qu'une clause de sécurité qui permet de restreindre l'accès à une partie seulement des entités. On peut par exemple restreindre l'accès aux archive pour un groupe selon le profil d'archivage ou le code d'accès, ou encore l'identifiant du service versant.



Gestion des sécurités

Seul un administrateur de l'application habilité peut accéder à la gestion des utilisateurs et des groupes pour les opérations d'ajout, de modification et éventuellement de suppression.

Toutes les opérations sur les données de sécurité sont dûment historisées dans le journal d'audit de l'application.

Protection contre les intrusions

Maarch RM permet d'activer un outil de contrôle des données échangées lors des communications avec les logiciels clients tels que les navigateurs internet. Ce composant technique détecte les tentatives d'injection SQL ou le Cross-Site-Scripting.

Journalisation

Maarch RM conserve un historique des événements survenus dans l'application et sur les archives dans deux journaux:

- Le journal d'audit du système
- Le journal du cycle de vie des archives

Chaque événement est horodaté afin de le positionner dans le temps par rapport aux autres événements. Il présente toutes les informations nécessaires à son exploitation: objet concerné, utilisateur, type d'opération, message explicite, etc.

L'accès aux journaux pour consultation est réservé aux personnes habilitées par le système de gestion des autorisations selon les deux axes explicités dans le chapitre consacré aux sécurités:

- L'attribution du privilège d'accéder aux fonctions et commandes
- La définition du périmètre de données accessible

Conservation sécurisée des journaux

Maarch RM consigne au fil de l'eau dans la base de données les événements de l'application et les événements du cycle de vie de l'archive. Ceci permet aux personnes habilitées d'exploiter facilement les journaux:

- Rechercher des événements sur des critères de type, de date, d'archive concernée, etc.
- Consulter la séquence des événements classés par horodatage
- Consulter les événements liés à une archive en particulier

Une fois par jour, la procédure d'archivage des journaux est exécutée afin d'assurer leur conservation sécurisée. Elle exporte de la base de données tous les événements consignés durant la journée d'exploitation vers deux fichiers au format XML, l'un pour l'audit de l'application, l'autre pour le cycle de vie de l'archive.

Le journal du cycle de vie de l'archive est chaîné, l'empreinte numérique correspondant au précédent fichier XML de journal est inscrite au début du nouveau fichier de journal produit. On peut ainsi s'assurer de la continuité de l'historique des événements.

Les fichiers de journaux produits sont versés dans le système d'archivage avec un jeu de métadonnées descriptives spécifiques à l'archivage des logs:

Donnée	Description
type	Type de log: journal du cycle de vie, audit ou autre
fromDate	Date et heure de début des événements historisés
toDate	Date et heure de fin des événements historisés
processId	Identifiant du processus (pour les logs système, de batch, etc)
processName	Nom du processus (pour les logs système, de batch, etc)

Les fichiers de journaux sont conservés selon les mêmes conditions que les archives : scellement par empreinte numérique, redondance du stockage, obligation de métadonnées de gestion pour la conservation et la sécurité.

Journal du cycle de vie des archives

Le journal de cycle de vie des archives est alimenté dès qu?une opération de création, de modification ou de suppression d?un profil d?archivage est effectuée ou qu?une nouvelle attestation électronique est générée pour une archive.

Le journal du cycle de vie des archives peut être consulté partiellement ou dans son intégralité par les personnes habilitées :

- Possédant le privilège de recherche/consultation du journal du cycle de vie
- Ayant un accès aux données du journal via une règle d'accès basée sur le code d'accès

Les informations conservées dans le journal du cycle de vie des archives sont les suivantes:

Donnée	Description
timestamp	Horodatage de l'événement
eventType	Type d'événement parmi: dépôt, modification, communication, restitution, destruction, modification de profil, ajout de profil, suppression de profil
journalId	Identifiant du receveur de journal dans lequel est tracé l'événement
archiveId	Identifiant de l'archive ou du profil concerné
accessCode	Code d'accès porté par l'archive ou le profil, qui permet de définir les droits des personnes à consulter l'événement
certificate	Attestation associée à l'événement sur archive

Journal des événements

Le journal d'audit de l'application consigne toutes les opérations effectuées par les utilisateurs ou par le système,et notifiées dans l'application comme étant significatives, notamment :

- Connexion d'un utilisateur
- Tentative de connexion infructueuse
- Ajout, modification ou suppression dans les référentiels via les panneaux d'administration
- Étapes du cycle de vie des archives
- Étapes des traitements par lot sur un élément à traiter
- Stockage sur support d'un document numérique
- Etc.

Chaque événement est consigné dans le journal d'audit selon le format suivant :

Donnée	Description
timestamp	Horodatage de l'événement
eventType	Type d'événement, fourni par le paquet métier
objectClass	Classe de l'entité sur laquelle porte l'événement
objectId	Identifiant de l'entité que laquelle porte l'événement
userId	Identifiant de l'utilisateur
message	Message intelligible par l'opérateur

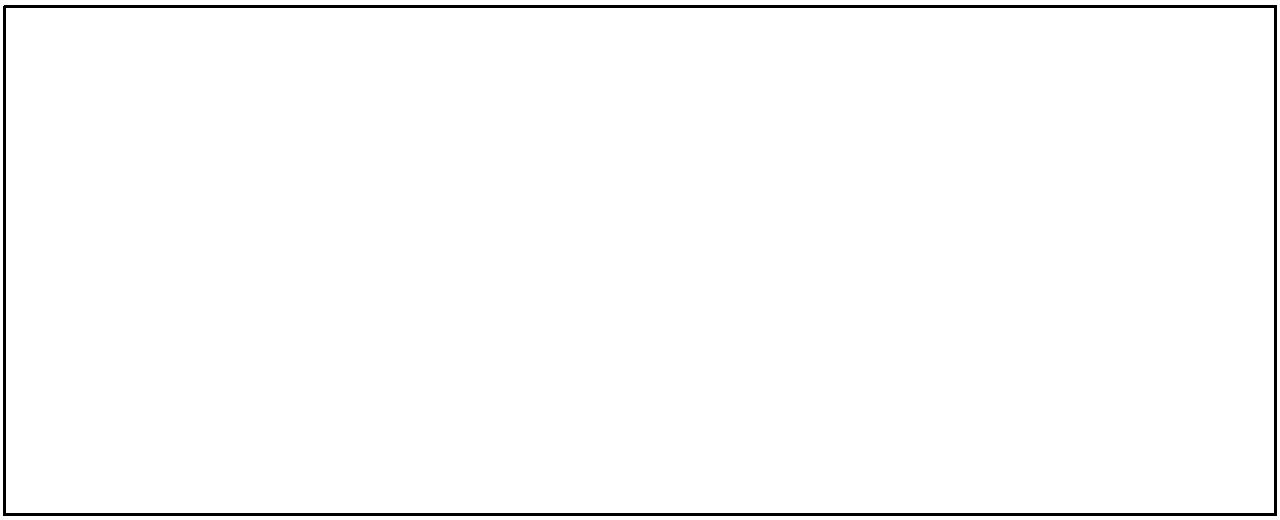
Exploitation des archives

Communication

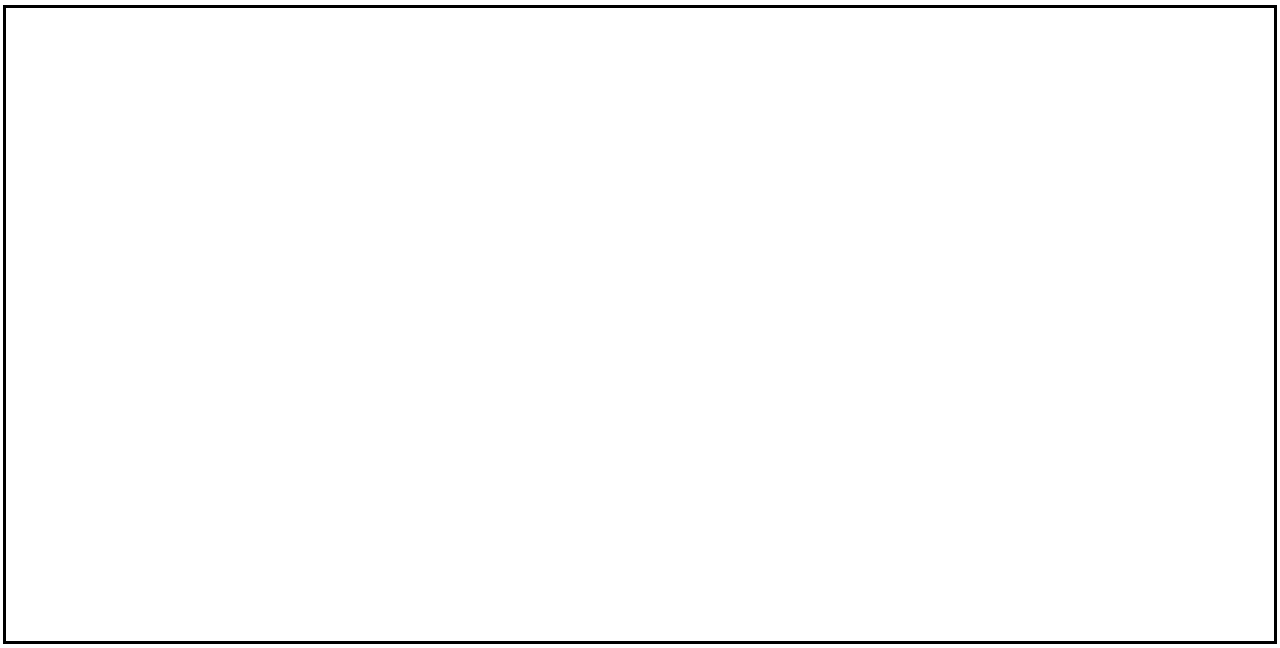
Les archives numériques sont accessibles par des écrans de recherche multicritère adaptés au domaine métier :

- Archives publiques
- Archives métier (factures, RH, dossiers, etc)

Exemple d'écran de recherche pour les archives publiques :

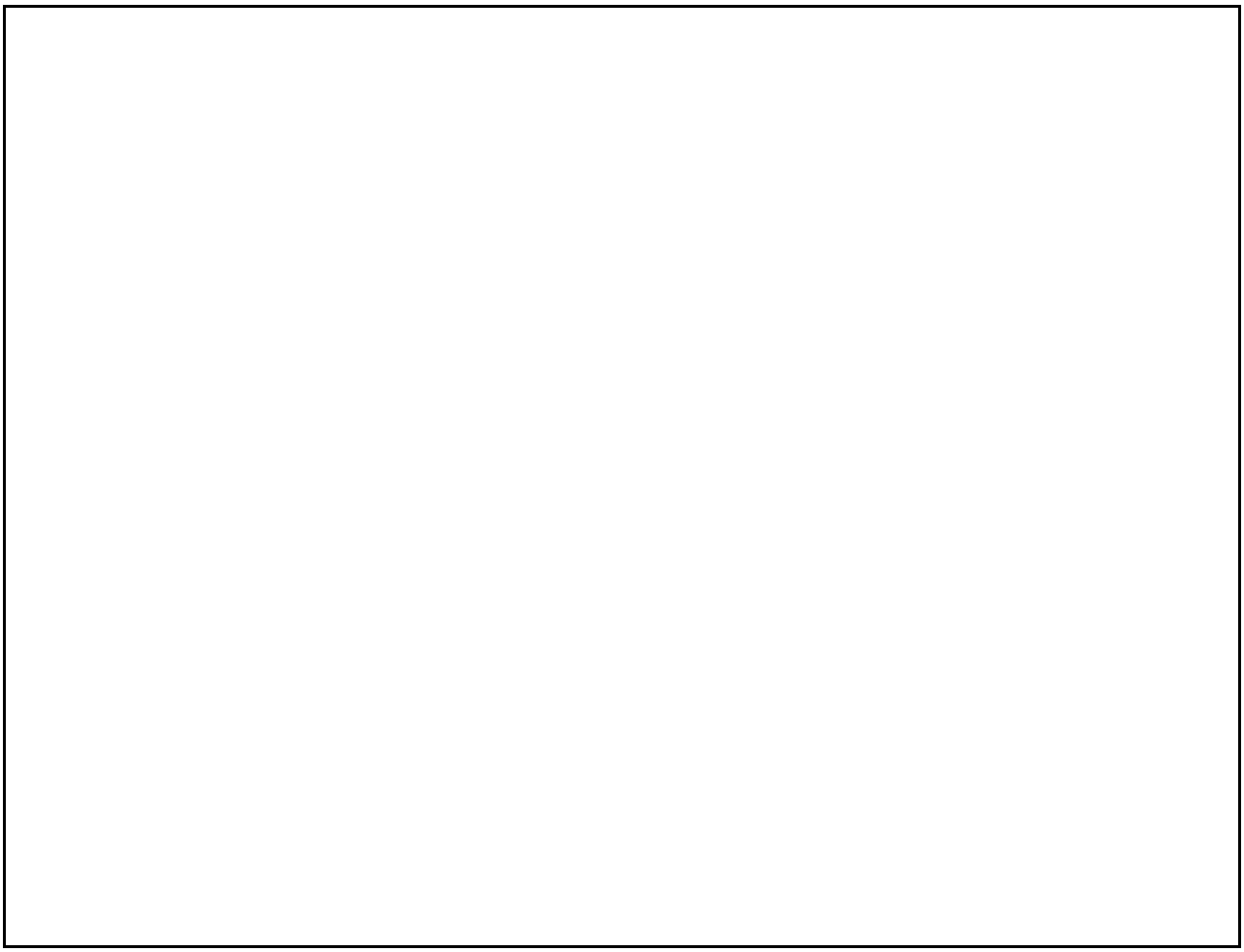


MaarchRM renvoie des listes de résultats filtrables et paginées, conçues pour une occupation de la bande passante et des performances optimales.



Des boutons de commande affichent une vue complète des propriétés de l'archive :

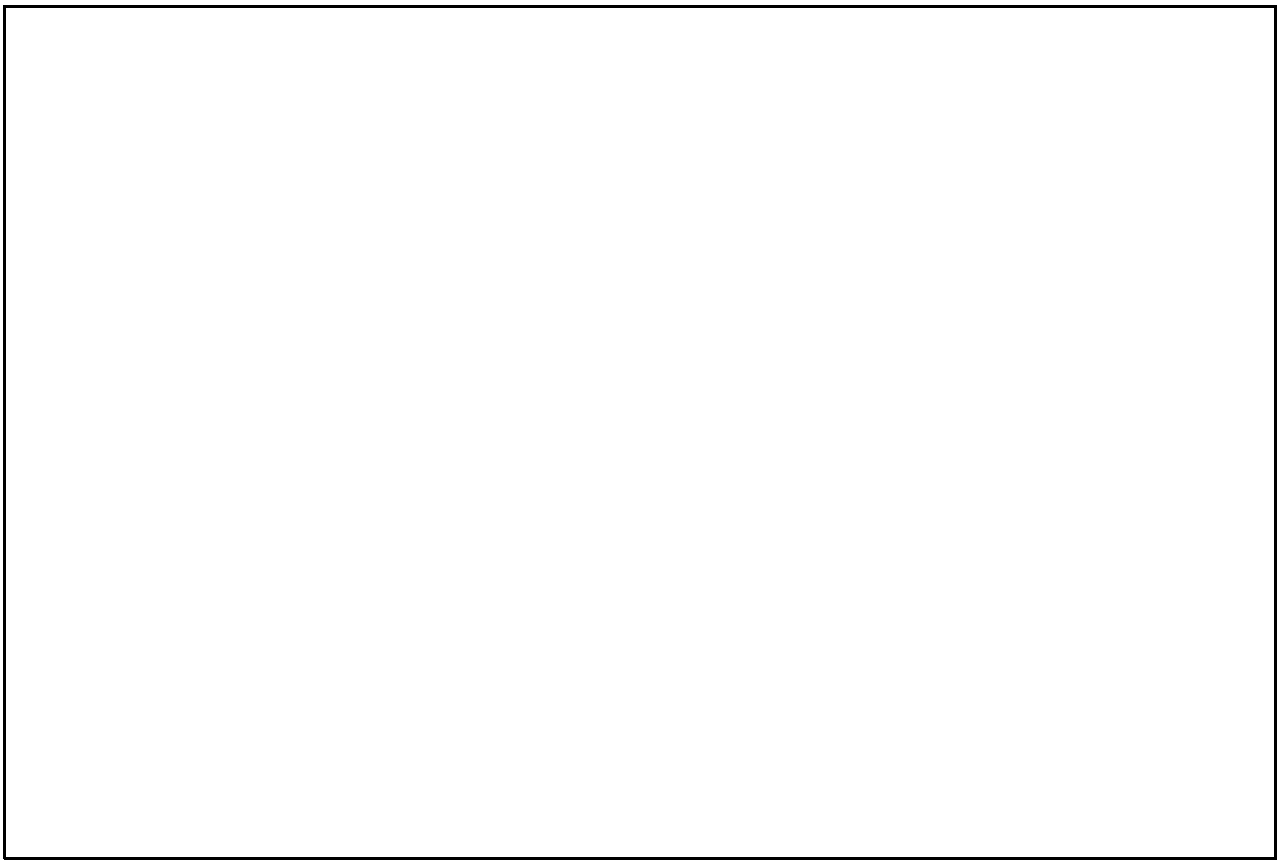
1. Informations archivistiques
2. Descripteurs fonctionnels (métadonnées métier)
3. Contenu
4. Événements du cycle de vie



Gestion des archives

MaarchRM dispose de tous les outils pour la gestion du cycle de vie de l'archive.

La modification des règles de conservation est par exemple possible en disposant des droits relatifs. Elle permet de modifier au niveau de l'archive la règle de conservation établie au versement. Toute modification fait l'objet d'un enregistrement dans le journal de cycle de vie.



Les demandes d'élimination se font au travers de bordereaux SEDA ou MEDONA, en suivant différentes étapes de validation (Archiviste ? Producteur ? (CST ?) Archiviste), et sous couvert éventuel du Contrôle Scientifique et Technique (CST).