POLITIQUE D'ARCHIVAGE DU SAE

AUTEUR(S)	:	Guillaume Bailleul
N° DE DOCUMENT	:	WLM-ARC-F210
VERSION	:	1.2
STATUT	:	Final
SOURCE	:	Worldline
DATE DU DOCUMENT	:	23 avril 2019
NOMBRE DE PAGES	:	27
PROPRIETAIRE	:	Comité Mediacert

TSP Media Cert

Digitally signed by TSP MediaCert
DN: CN=TSP MediaCert, O=Worldline, E=dl-mediacert-tsp@worldline.com, C=FR
Reason: I am approving this document
Location:
Date: 2019-04-26 11:24:56

Rôle	Nom	Signature	Date
Relecteur 1 – Resp adjoint TSP	Fanny Lesecq	Fanny Lesecq	23/04/2019
Relecteur 2 – RSSI	Didier Sobkowiak	Didier Sobkowiak	23/04/2019
Fonction d'assurance qualité	Fanny Lesecq	Fanny Lesecq	23/04/2019
Propriétaire du document	Comité Mediacert	Guillaume Bailleul	23/04/2019
Approbateur – Resp TSP	Guillaume Bailleul	Guillaume Bailleul	23/04/2019

Table des matières

Liste des modifications

Version	Date	Description	Auteur(s)
1.0	07/12/2012	Version initiale	Jean Jacques Milhem
1.1	10/05/2018-12/10/2018	Relecture et amendement	Guillaume Bailleul
1.2	12/12/2018 – 31/03/2019	Amendements suite à l'audit de certification	Guillaume Bailleul

1 Introduction

1.1 Objet du document

Ce document décrit la Politique d'Archivage (PA) de WL e-archiving, Système d'Archivage Electronique (SAE) hébergé par Worldline.
Ce document sert de base à l'élaboration des PA à mettre en œuvre dans le cadre de la fourniture d'un Service d'Archivage.
L'objectif final de la PA est de permettre aux Archives électroniques gérées par le SAE qui ont une valeur juridique initiale d'être considérées comme fiables, c'est à dire de conserver leur intégrité et garantir qu'ils sont conformes aux documents d'origine, tant en terme probatoire qu'en terme de validité et ce pendant toute leur durée de conservation au sein de WL e-archiving.

1.2 Nom et codification

Le présent document est intitulé « Politique d'Archivage de WL e-archiving. ». Il est référencé dans le système documentaire sous la référence WLM-ARC-F210. La présente Politique d'Archivage est identifiée par l'OID 1.2.250.1.111.20.4.1.

1.3 Bibliographie

1.3.1 Références externes

Référence	Description
[GA Z42-019]	GA Z42-019 (Juin 2010) AFNOR Guide d'application de la NF Z 42-013
[NF 461]	NF 461 (Septembre 2015) AFNOR Certification Règles de certification d'un système d'archivage électronique
[NF Z 42-013]	NF Z 42-013 (Mars 2009) AFNOR Archivage électronique : spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes
[RGPD]	Règlement Général sur la Protection des Données Parlement Européen et Conseil de l'UE
[ISO 9001]	ISO 9001 (2015) Systèmes de management de la qualité
[ISO 27001]	ISO 27001 (2013) Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

1.3.2 Références internes

Référence	Description
[AR]	Analyse de Risque de la plateforme d'Archivage Service d'Archivage Electronique Référence : WLS-ARC-F191
[DDTS]	Dossier de Description Technique du Système SAE WA

Référence	Description
	Service d'Archivage Electronique Référence : WLS-ARC-F208
[PAQ]	Plan d'Assurance Qualité de la Software Factory TSP Mediacert Référence : WLM-SFY-F122
[PG]	Politique Générale du TSP MediaCert TSP Mediacert Référence : WLM-TSP-F094 OID : 1.2.250.1.111.20.1.1
[PSI]	Politique de Sécurité de l'Information de Worldline France Worldline France Référence : WLM-SEC-F002
[PSO]	Politique de Sécurité Opérationnelle Service d'Archivage Electronique Référence : WLS-ARC-F206
[SMQ]	Système de Management de la Qualité Worldline Worldline France Référence : WLM-QUA-F000
[SMSI]	Système de Management de Sécurité de l'information Worldline Worldline France Référence : WLM-SEC-F002

2 Définitions

2.1 Définitions

2.1.1 Document Numérique

Le Document Numérique est un ensemble compose d'un contenu, d'une structure logique et d'attributs de presentation. Cet ensemble permet la representation du document sous une forme intelligible par l'homme. Le document numérique s'entend au sens de la definition fournie dans la [NF Z 42-013].

2.1.2 Archive

Une Archive est un paquet d'informations composé d'un ou plusieurs fichiers informatiques reçu, conservé et communiqué par WL e-archiving. Le paquet d'informations est l'association du contenu et de ses attributs de pérennisation précisant sa provenance, son contexte, son identification et les attributs permettant le contrôle de son intégrité. On parle également d'Archive électronique.

2.1.3 Métadonnées

Ensemble structuré d'informations techniques, de gestion et de description attaché à un document servant à décrire les caractéristiques de ce document en vue de faciliter son repérage, sa gestion, sa consultation, son usage ou sa préservation.

2.1.4 Archivage Electronique

[NF Z42-013]L'Archivage Electronique est défini comme l'ensemble des actions visant à identifier, recueillir, classer, conserver, communiquer et restituer des documents électroniques, pour la durée nécessaire à la satisfaction des obligations légales ou pour des besoins d'informations ou à des fins patrimoniales.

2.1.5 Autorité d'Archivage

L'Autorité d'Archivage est l'entité métier responsable de la gestion du service d'Archives. Cette entité propose des services, qui peuvent être mutualisés, à partir d'une prestation globale d'Archivage électronique réalisée par un Tiers Archiveur.

2.1.6 Client

Le Client est le maître d'ouvrage, ou encore, pour le secteur public, l'entité qui peut avoir une structure juridique de groupement pour proposer des services mutualisés d'archivage à ses membres adhérents pour leurs propres autorités d'archivage.

2.1.7 Empreinte

L'Empreinte est le résultat de l'application d'une fonction de mise sous forme canonique puis d'une fonction de hachage appliquées sur un document. Ce résultat est un ensemble d'octets permettant de caractériser un document. Toute modification du document entrainera une empreinte différente qui révélera la modification par comparaison avec la première empreinte.

2.1.8 Fichier de Description de l'Archive

Le Fichier de Description de l'Archive désigne un fichier constitutif de l'Archive contenant l'ensemble des métadonnées de l'Archive ou des documents contenu dans l'Archive.

2.1.9 Horodatage d'un document

L'**horodatage** (en anglais *timestamping*) est un mécanisme qui consiste à associer une date et une heure à un événement, un documentou une donnée informatique. Il a généralement pour but d'enregistrer l'instant auquel une opération a été effectuée.

2.1.10 Identifiant Unique d'Archive

L'Identifiant Unique d'Archive (IUA) est l'identifiant de celle-ci dont l'unicité est garantie pour une Convention d'Archivage donnée.
La paire composée de l'identifiant de Convention d'Archivage et de l'IUA est unique sur l'ensemble de la plateforme du Service d'Archivage.

2.1.11 Restitution

Ensemble des mécanismes permettant de rechercher et de remettre les documents numériques à l'organisme qui les a produits ou à ses mandants, puis de les détruire au sein de son système d'archivage.

2.1.12 Versement

Transmission par un client d'un document numérique au SAE.

2.1.13 Service d'Archivage

Le Service d'Archivage désigne l'entité destinataire du versement. Il assure la gestion des Archives versées par les Services Versants, destinées à être communiquées aux Usagers des Services Versants / Producteurs dans le respect des délais de communicabilité. Le Service d'Archivage assure également une mission de conseil auprès des Services Versants ou des Services Producteurs.

2.1.14 Service de Contrôle

Dans le domaine public, le Service de Contrôle est composé de personnes habilitées par les textes législatifs et réglementaires en vigueur, à contrôler les Archives publiques, notamment de la façon dont les Autorités d'Archivage s'acquittent de leur mission (création, versement, stockage, communication des Archives, administration). Les contrôleurs doivent bénéficier d'un accès à WL e-archiving.

2.1.15 Service Producteur

Le Service Producteur est l'entité qui a initialement reçu ou produit l'Archive et qui en est propriétaire. La notion de Service Producteur est propre au domaine public.

2.1.16 Service Versant

Le Service Versant est l'entité qui verse un paquet d'informations à un Service d'Archivage.

2.1.17 Usager

L'Usager est une personne physique ou morale autorisée à consulter les Archives conservées sur le SAE dans le respect de la législation applicable en matière de communication des Archives.

2.1.18 Utilisateur

L'Utilisateur désigne toute personne physique ou morale autorisée à utiliser WL e-archiving.

2.1.19 Tiers Archiveur

Un Tiers Archiveur est une personne physique ou morale en charge, pour le compte de tiers, d'offrir les fonctionnalités du Service d'Archivage électronique, à savoir : réception des dépôts, conservation, communication, destruction ou restitution. Les conditions de réalisation de ces services doivent être définies dans un contrat de services conforme aux recommandations de la norme [NF Z42-013] et du guide d'application [GA Z42-019]. Dans la présente PA, il s'agit de Worldline.

2.1.20 Convention d'Archivage

La Convention d'Archivage est un document décrivant l'ensemble des règles de transfert, contrôle et conservation des archives. Ce document est partagé entre le client et le Tiers Archiveur.
Chaque Convention d'Archivage est archivée au sein de WL e-archiving, pour une durée indéterminée.

2.1.21 Plan de Continuité d'Activité (PCA)

Ensemble de mesures visant à assurer, selon divers scénarios de crise, y compris face à des chocs extrêmes, le maintien, le cas échéant de façon temporaire selon un mode dégradé, des prestations de services essentielles de l'entreprise puis la reprise planifiée des activités.

2.2 Abréviations et acronymes

Acronyme	Description
AA	Autorité d'Archivage
IUA	Identifiant Unique d'Archive
IUAA	Identifiant Unique d'Agrément d'Archivage
FDA	Fichier de Description de l'Archive
OH	Operational Handbook
PA	Politique d'Archivage
PSO	Politique de Sécurité Opérationnelle
SAE	Système d'Archivage Electronique, correspond à WL e-archiving
SOP	Standard Operation Procedure
SP	Service Producteur
SV	Service Versant
TA	Tiers Archiveur

3 Fonctionnalités mises en œuvre

Le Tiers Archiveur propose un Service d'Archivage Electronique de documents numériques nommé WL e-archiving. Ce service est sécurisé. Il s'engage auprès des Clients ayant souscrit au service à :

- à intégrer dans le SAE, en sécurisant le versement, les documents numériques ;
- conserver ces documents et s'assurer de pouvoir garantir pendant la durée de conservation convenue contractuellement:
  - leur sécurité ;
  - leur pérennité ;
  - leur intégrité ;
  - leur traçabilité ;
  - leur disponibilité et accessibilité en ligne aux Usagers autorisés ;
- respecter les demandes du Client en matière de réversibilité en fin de contrat conformément aux accords contractuels entre les parties.

WL e-archiving est également nommé Service d'Archivage dans le présent document.

3.1 Versement

3.1.1 Contrôle de l'origine du versement

Le Tiers Archiveur s'assure de la provenance des Documents Numériques. Le Tiers Archiveur référence les sources de documents pour chacun de ses Clients.
Le Tiers Archiveur sécurise les moyens de communication. Il s'assure de la confidentialité des échanges et de l'authenticité des sources.

3.1.2 Documents numérique et métadonnées

Les documents numériques destinés à être conservés dans le temps sont accompagnés d'un ensemble de métadonnées nécessaire à cette conservation. Les documents numériques sont également appelés documents.

3.1.3 Identifiant unique de l'Archive

Se référer au chapitre Définitions.

3.1.4 Validation de format

WL e-archiving garantit la conservation des documents. Afin de renforcer les capacités de conservation d'un document numérique, le Service d'Archivage propose un service facultatif de validation de format.

La Convention de Service définit la liste des formats validés par le Tiers Archiveur.

3.1.5 Horodatage

La date (date et heure) de création de l'Archive est conservée et scellée dans l'Archive. Cette date repose sur un service de temps normalisé, disposant de plusieurs sources de temps.

3.1.6 Scellement de l'Archive

Les Archives sont scellées par un moyen cryptographique permettant de garantir l'intégrité des documents de l'Archive et des métadonnées la décrivant.
Les calculs d'Empreinte de l'Archive et des documents constitutifs de l'Archive sont réalisés au moyen d'une fonction de hachage cryptographique.
L'empreinte est scellée. Se référer au chapitre Scellement du présent document.
Le scellement de l'Archive contient une contremarque de temps permettant de prouver l'existence de l'Archive à une date donnée.
L'Archive scellée contient, entre autres les attributs suivantes :

- l'identifiant unique de l'Archive ;
- la date de création de l'Archive ;
- les Empreintes de chacun des documents de l'Archive ;
- les métadonnées descriptives de chacun des documents de l'Archive ;
- les métadonnées descriptives de l'Archive.

3.1.7 Indexation de l'Archive

Lors de la constitution de l'Archive, l'ensemble des métadonnées est extrait afin de permettre l'indexation de l'Archive et de simplifier des recherches.
Les metadonnées de cet ensemble pourront être utilisées pour faire des recherches lors de la consultation d'Archives (voir 3.2.2).

3.1.8 Sécurisation du stockage de l'Archive

Suite à sa constitution, l'Archive est déposée sur plusieurs sites distants afin de garantir sa sécurisation. Les solutions de stockage employées sur chaque site garantissent une multiple copie de archive afin de sécuriser le stockage contre les risques de panne matérielle.
Une copie de sauvegarde, asynchrone, est effectuée sur une solution de sauvegarde.
Le Service d'Archivage propose un acquittement fonctionnel garantissant la sécurisation et le stockage de l'Archive.

3.1.9 Preuve de dépôt de l'Archive

3.1.9.1 Accusé de réception technique

Lors du versement, un accusé de réception technique est retourné par le Service d'Archivage. Il permet d'attester que l'Archive a été complétement reçue et que la demande d'archivage est complète et cohérente.
La réception de cet avis de réception garantit que l'Archive a été correctement **constituée et scellée**. L'Archive devient donc accessible par son propriétaire au travers des outils prévus à cet effet.
Cet accusé de réception technique contient, entre autres, les informations suivantes :

- L'identifiant unique d'Archive ;
- L'heure de dépôt;
- Le statut de l'archive;
- La localisation de l'archive;

3.1.9.2 Accusé de réception fonctionnel

Après versement, un accusé de réception fonctionnel est disponible sur demande. Il est accessible en utilisant l'identifiant unique de l'Archive et retourne les mêmes informations que l'accusé de réception technique. Il garantit la **sécurisation** de l'Archive, c'est-à-dire que l'Archive est stockée sur les sites définis par cette politique d'archivage.
Le déposant dispose alors, pour chaque archive, de la preuve de dépôt.

3.2 Recherche

WL e-archiving propose deux types de recherche :

- recherche par Identifiant Unique d'Archive ;
- recherche multicritère.

3.2.1 Recherche par Identifiant Unique d'Archive

WL e-archiving propose un moyen de recherche des Archives en fonction de leur IUA. L'outil de recherche n'est accessible qu'aux Utilisateurs définis par le Client.
Pour un Utilisateur donné, les résultats des recherches ne contiennent que les Archives auxquelles il a accès conformément à la Convention d'Archivage.

3.2.2 Recherche multicritère sur métadonnée

WL e-archiving propose un moyen de rechercher des Archives en fonction des métadonnées associées à l'Archive ou aux contenus lors du dépôt. L'outil de recherche n'est accessible qu'aux Utilisateurs définis par le Client.
Pour un Utilisateur donné, les résultats des recherches ne contiennent que les Archives auxquelles il a accès conformément à la Convention d'Archivage.

3.3 Communication

3.3.1 Communication unitaire

Quand il est en possession d'un IUA, l'Utilisateur peut récupérer les informations suivantes :

- le journal de l'Archive ;
- les attributs de scellement de l'Archive ;
- la description de l'Archive ;
- chacun des contenus constitutifs de l'Archive.

Toutes ces informations sont téléchargeables à partir d'une application cliente authentifiée auprès du Service d'Archivage.

3.3.2 Communication en nombre

Sur demande particulière et aux conditions prévues par la convention de service, il est possible de demander au Service d'Archivage une communication d'un nombre important d'Archives.

3.4 Modification d'Archive

WL e-archiving ne permet pas la modification de l'Archive et garantit son intégrité. Néanmoins, dans certains contextes, il peut être nécessaire de faire évoluer le contenu. Le Service d'Archivage permet la dépose d'une nouvelle révision d'Archive faisant référence à la version précédente. Dès lors, par défaut, la dernière révision de l'Archive sera retournée lors de la communication.
Optionnellement, et suivant la convention d'archivage, les versions précédentes de l'Archive peuvent être supprimées afin d'assurer la compatibilité du service au Règlement Général de Protection des Données personnelles (RGPD). Le journal d'Archive garde alors toute trace des suppressions de versions précédentes.

3.5 Restitution

Les Archives pourront à la demande du Client être restituées en totalité. Les modalités d'application de cette restitution suivront les contraintes et préconisations de la restitution en nombre (voir 3.3.2).
La définition du support de restitution est définie dans la convention de service et est faite en accord avec le Client.
Le format de restitution par défaut est un format spécifique WL e-archiving inspiré de formats reconnus.

3.6 Fin de vie de l'Archive

La convention de service prévoit une durée de service et une durée de conservation des documents archivés.

3.7 Destruction d'Archive exceptionnelle

Le Client peut, sur demande expresse, demander la destruction d'Archives. Dans ce cas les Archives concernées par la destruction doivent être clairement identifiées. Une trace de la demande et de la suppression sera conservée par le Service d'Archivage.
La suppression d'une archive implique la suppression de ses métadonnées tout en conservant ses journaux.

3.7.1 Cycle de vie du service

Régulièrement les Archives sont vérifiées afin de constituer la liste des Archives dont la durée de vie (durée de conservation) arrive à échéance. Cette liste est communiquée au responsable (Client) des Archives qui, pour l'ensemble ou pour chacune d'elle, déterminera l'étape suivante de la vie de l'Archive, soit autoriser la destruction ou opérer un allongement de la durée de vie de l'Archive.
Le Service d'Archivage garde la trace des choix et réalise les actions nécessaires.

3.7.2 Conservation

3.7.2.1 Durée de conservation

La durée de conservation est définie dans le contrat entre le Client et le Service d'Archivage. Pour chaque type d'Archive défini dans la convention d'archivage une durée d'archivage est définie.
En cas de fin de contrat, une restitution complète des Archives sera planifiée (voir 3.5).

3.7.2.2 Consultation au-delà de la durée du service

Si cela est prévu au contrat, un accès aux Archives pourra être maintenu après la cessation du service de dépose. Le Client pourra accéder aux Archives suivant les conditions prévues dans le contrat.
Le Client pourra demander la restitution suivant les conditions prévues au contrat et suivant les contraintes définies dans la politique d'archivage (voir 3.5).

3.8 Exploitation

3.8.1 Procédures et règles d'exploitation

L'ensemble des procédures et des règles de WL e-archiving est documenté. Conformément aux règles du [SMSI], elles font l'objet d'une relecture régulière et d'une amélioration continue.

3.8.2 Développement des systèmes

Les activités de développement, d'intégration et de test de nouveaux systèmes, ou de nouvelles versions de systèmes existants, sont séparées (tâches et environnement physique) des activités d'exploitation opérationnelle. Les livrables développés sont installés en production à partir du référentiel documenté.

3.8.3 Maintenance des systèmes

Les opérations de maintenance sur les systèmes en exploitation sont préparées et enregistrées. Les procédures d'intervention sur les systèmes (à chaud ou à froid) sont formalisées et les éléments objet de la maintenance sont préalablement testés dans un environnement séparé avant leur mise en exploitation.
Les opérations de maintenance sont réalisées sous le contrôle de personnels ayant des rôles de confiance, tels que définis dans le document de Politique Générale [PG].
Les opérations de maintenance font l'objet d'une traçabilité complète.

3.8.4 Gestion des supports

Les supports de stockage (informatiques et papiers) font l'objet d'une gestion formalisée conforme aux besoins de sécurité et de qualité des services du Trust Service Provider (TSP) Mediacert. Les règles applicables aux services du TSP Mediacert sont énoncées dans le document de Politique Générale [PG].
Notamment, la réutilisation / mise au rebut / sortie des locaux (maintenance) de supports fait l'objet de procédures strictes liées à l'effacement sécurisé des fichiers contenues sur le support ou la destruction physique du support.

3.8.5 Reporting

Le Service d'Archivage met à disposition des Clients un rapport d'activité mensuel contenant les mesures nécessaires au pilotage de l'activité. Seront notamment présents :

- le nombre d'Archives déposées sur la période ;
- la taille de l'espace de stockage utilisé.

3.9 Attestations disponibles

Pour chaque archive présente dans le système d'archivage, le Tiers Archiveur peut fournir plusieurs types d'attestation afin d'atester du fonctionnement du système et du respect du cycle de vie de l'archive.

Ces attestations sont les suivantes:

- L'attestation de copie d'une archive fournie l'ensemble des éléments nécessaires pour s'assurer que l'archive communiquée est compléte et conforme.
- L'attestation de suppression d'archive permet de tracer les suppressions d'archives sur la plateforme d'archivage.
- Les attestations de création, suppression et modification d'une convention d'archivage permettent de retracer le cycle de vie des conventions d'archivage d'un Client.

L'attestation d'éxécution de contrôle de fond rend compte des controles en continue du fond d'archive.
Les attestations du cycle de vie des archives sont regroupées et signées périodiquement à intervalle fixe et paramétrable pour constituer le journal.

4 Principes organisationnels

4.1 Politique d'archivage

4.1.1 Diffusion de la Politique d'Archivage

La Politique d'Archivage est un document classifié public diffusé, à la demande, à l'ensemble des parties concernées par le SAE sur l'espace documentaire du projet.

4.1.2 Evolution de la Politique d'Archivage

La Politique d'Archivage est tenue à jour pour toute évolution du SAE. Les Déclarations de Pratiques d'Archivage (DPA) doivent être maintenues conformes à la PA en vigueur.
La PA est revue, a minima, annuellement (cf. action récurrente WLP-TSP-F106).

4.1.3 Contrôle d'application de la Politique d'Archivage

Le Tiers Archiveur prévoit et met en œuvre les procédures et moyens nécessaires pour s'assurer de l'application de la PA.

4.2 Conservation des Archives

Durant toute la durée de conservation, le Tiers Archiveur pourra présenter l'Archive ou une partie de l'Archive référencée par un Identifiant Unique d'Archive (IUA).
Pour s'assurer de la conservation, plusieurs copies de l'Archive sont réalisées suivant les règles spécifiées dans la Déclaration des Pratiques d'Archivage.
Un acquittement technique est émis dès la réception complète de l'Archive et son scellement.
Un acquittement fonctionnel est émis dès que le nombre de copie correspond aux règles définies dans la DPA.
Des processus réguliers s'assurent, par échantillonnage de l'intégrité des Archives conservées par le Tiers Archiveur.

4.2.1 Disponibilité du service

Le Service d'Archivage WL e-archiving est prévu pour une disponibilité en continu, 24 heures sur 24 et 7 jours sur 7 en dehors des périodes de maintenance planifiées. Le taux de disponibilité fournit est de 99,5 %. L'architecture technique du SAE, définie dans le [DDTS], permet d'assurer un haut niveau de disponibilité.

4.2.2 Sécurité des archives

Les aspects primordiaux de la sécurisation du stockage de documents numériques sont également traités :

- pérennité ;
- intégrité ;
- confidentialité ;
- traçabilité ;
- réversibilité.

4.2.2.1 Pérennité

Le système de stockage des documents utilisé s'assure en permanence du bon fonctionnement de chaque composant hardware de la plateforme. En cas de défaillance d'un élément matériel, les principes de redondance mis en place permettent d'assurer un accès continu à l'archive malgré la panne et un retour au nombre de copie nécessaire après le remplacement de l'élément défectueux.

4.2.2.2 Intégrité

Le scellement de l'Archive ainsi que les Empreintes numériques des différents constituants de l'Archive sont vérifiés régulièrement par un contrôle en continu du Système d'Archivage Electronique.

4.2.2.3 Confidentialité

Le Tiers Archiveur s'engage à ne pas analyser les informations contenues dans les documents archivés.
Selon la Convention d'Archivage de l'Autorité d'Archivage, des validateurs de format peuvent être utilisés pour s'assurer de la validité du format du document déposé. Dans ce cas, seule la structure du document est analysée, le contenu n'est ni extrait ni analysé.
WL e-archiving met en place du cloisonnement et une gestion des habilitations afin de s'assurer que seuls les Utilisateurs autorisés accèdent aux Archives.
Dans certains cas, le Service Versant peut chiffrer les documents avant leur dépose dans l'archivage. Ce principe permet une confidentialité renforcée mais implique un contrôle par le Client du cycle de vie des clés de chiffrement utilisées.
Les archives sont cryptés avant leur envoi au service de stockage.

4.2.2.4 Traçabilité

Le Service d'Archivage assure la traçabilité par la mise en place d'un système de journalisation. Les événements du système sont enregistrés dans différents journaux.
Les types de journaux suivants sont définis dans le système :

- journal du cycle de vie des Archives ;
- journal des événements ;
- journal système.

Journal du cycle de vie de l'Archive

Le système enregistre pour chaque Archive les événements concernant son cycle de vie. On y retrouve, entre autres, les événements suivants :

- dépôt de l'Archive ;
- suppression de l'Archive ;
- modification de la durée de vie de l'Archive ;
- restitution de l'Archive.

Le journal d'une Archive est accessible aux Usagers du Service d'Archivage suivant les mêmes règles que l'accès aux Archives.

Journal des événements

Il existe un système d'enregistrement permettant de répertorier les événements concernant les ressources de la plateforme de WL e-archiving. Y sont répertoriés les événements suivants :

- ajout de matériel ;
- remplacement de matériel ;
- maintenance.

Ces éléments sont accessibles aux opérateurs de la plateforme.

Journal système

Les journaux systèmes sont un sous ensemble des journaux d'événement. Ils sont traités avec le même niveau de sécurité que les journaux d'événements. Ils enregistrent l'ensemble des événements de la plateforme. Y sont répertoriés, entre autres :

- les actions de sécurité ;
- les évolutions du système ;
- les accès à la plateforme.

Ces journaux permettent une analyse a posteriori et une reconstitution de l'historique de la plateforme.

4.2.2.5 Réversibilité

WL e-archiving respecte le principe de réversibilité (voir 3.5). Les documents archivés ainsi que leurs métadonnées ne sont pas modifiés par les processus du Service d'Archivage.
Le Service d'Archivage permet donc la restitution des documents et de leurs métadonnées sans aucune transformation interne.
Les Archives seront restituées sous un format spécifique au Service d'Archivage inspiré par les standards du marché. Le support de la restitution est défini dans le contrat.
Le processus de restitution sera conduit suivant les conditions prévues dans le contrat.

5 Principes de mise en œuvre

La sécurité est un des points crucial de WL e-archiving. La sécurité du Système d'information repose sur les règles générales mises en place dans l'entreprise pour obtenir les certifications nécessaires à ce genre d'activité. La sécurité des systèmes concerne :

- la sécurisation des réseaux (filtrage, utilisation de réseaux privés) ;
- la sécurisation des accès physiques ;
- la sécurisation des accès logiques (authentification personnelle, utilisation de certificats, politique de sécurité des accès) ;
- la sécurisation des échanges (utilisation de transport chiffré, HTTPS, TLS) ;
- la sécurisation de l'exploitation (définition de procédures, standardisation) ;
- la sécurisation des développements (application d'un Plan d'Assurance Qualité [PAQ]).

Les principes mis en œuvre par le Tiers Archiveur respectent l'ensemble des règles définies dans le [SMSI] et le [SMQ] de Worldline afin de garantir un niveau de sécurité suffisant. Les éléments suivants apportent des informations sur leur mise en œuvre.

5.1 Gestion de la documentation

La politique de gestion de la documentation mise en place est décrite dans la Politique Générale [PG] et est conforme au Système de Management de la qualité [SMQ] mis en place dans l'entreprise. L'entreprise est certifiée ISO 9001 [ISO 9001].

5.2 Gestion de la sécurité

La gestion de la sécurité repose sur la démarche globale mise en place pour l'ensemble des Services de Confiance du TSP Mediacert et sur une démarche similaire mise en place globalement dans l'entreprise.

5.2.1 Politique de sécurité de l'information

La politique mise en place est décrite dans la Politique Générale [PG] et est conforme au Système de Management de la Sécurité de l'Information [SMSI] mis en place dans l'entreprise. L'entreprise est certifiée ISO 27001 [ISO 27001]
Des règles spécifiques ou la spécialisation de certaines règles sont définies dans la Politique de Sécurité Opérationnelle [PSO] spécifique à WL e-archiving.
La politique de sécurité de l'information [PSI] exprime, entre autres, la description des relations avec les fournisseurs.

5.2.2 Planification de la continuité de l'activité (PCA)

Le Tiers Archiveur dispose d'un Plan de Continuité d'Activités (PCA) couvrant le périmètre du SAE. Le plan de continuité d'activité est réalisé en fonction de la nécessité du maintien de l'intégrité des Archives notamment la non-perte d'archives. Les procédures définies dans les différents plans

doivent permettre de maintenir les activités du Service d'Archivage conformément aux besoins en intégrité et en continuité.
Ce plan est régulièrement maintenu à jour. Il décrit un ensemble de mesures à appliquer avec pour objectif de maintenir, parfois sous une forme dégradée, les fonctionnalités de WL e-archiving.

5.2.3 Sécurité physique et environnementale

WL e-archiving repose sur une plateforme technique distribuée sur 3 sites distincts. Chaque site, dont l'un distant de plus de 400 kilomètres, dispose de leurs propres ressources de fonctionnement (climatisation, approvisionnement électrique, générateur de secours).

5.2.4 Sécurité des accès

5.2.4.1 Sécurité des accès physiques

Les accès aux actifs du SAE sont restreints et strictement contrôlés. Ils respectent des règles de sécurité définies dans la [PSI].

5.2.4.2 Sécurité des accès logiques

Les accès logiques aux actifs du SAE sont restreints et strictement contrôlés. Conformément à la [PSI], les accès sont nominatifs et tracés, et font l'objet d'une vérification régulière des autorisations d'accès.

5.2.5 Sécurité des matériels

Le choix des équipements, leurs installations et leur exploitation est fait en suivant les règles globales définies dans l'entreprise du Tiers Archiveur.

5.2.6 Gestion des incidents

Chaque entité intervenant dans le Service d'Archivage Electronique définit l'organisation et les procédures à suivre en cas d'incident de sécurité. Les procédures à suivre en cas d'incident sont définies dans des fiches Standard Operating Procedure (SOP).
La remontée d'information vers le Client suit les procédures standards définies dans l'entreprise.

5.2.7 Sécurité des logiciels

5.2.7.1 Développement logiciel

Le développement des logiciels suit les règles définies dans le Plan d'Assurance Qualité [PAQ] du département en charge de la plateforme d'archivage. Ce PAQ est compatible avec le Système de Management de la Qualité et le Système de Management de la Sécurité de l'Information de l'entreprise.

5.2.7.2 Intégration logicielle

Conformément aux bonnes pratiques de l'entreprise, le Tiers Archiveur met en œuvre des systèmes de test et d'acceptance afin de s'assurer du fonctionnement correct du service lors des évolutions des composants logiciels de celle-ci.

5.2.8 Sécurité du Système d'information

Conformément aux bonnes pratiques de l'entreprise et au [SMSI], le Tiers Archiveur met en œuvre une plateforme sécurisée en s'assurant de la redondance des éléments critiques dans le but d'assurer la sécurité du SAE.

5.2.9 Aspect Humains

5.2.9.1 Formation et Sensibilisation

Lors de son intégration, le nouveau personnel est formé et sensibilisé au caractère particulier de la sécurité du métier de Tiers Archiveur. Il est également sensibilisé à la politique de sécurité de l'entreprise.

5.2.9.2 Fiche de poste

Le travail de tout personnel intervenant sur WL e-archiving, à quelque niveau que ce soit (opérateur, administrateur, maintenance, etc.) fait l'objet d'une fiche de poste définissant les rôles, obligations et responsabilités du personnel concerné.

5.3 Echanges entre le Client et le Tiers Archiveur

5.3.1 Echange Projet

Le Tiers Archiveur ne propose pas de réunion de pilotage ou de suivi de projet centralisé sur le Service d'Archivage Electronique avec le Client. L'utilisation de l'archivage faisant généralement partie d'un projet informatique plus large, des instances pour ces suivis existent. Le suivi de l'archivage est intégré à chacune de ces instances. Sur demande du Client et des Chefs de Projets Worldline, un représentant du Tiers Archiveur pourra y participer.

5.3.2 Echange Technique

Les échanges de flux entre le Client et le Tiers Archiveur se font au travers de liens de communication sécurisés. La nature des liens seront définis d'un accord entre le Client et le Tiers Archiveur. La sécurisation des liens et le fruit d'un travail conjoint entre les équipes techniques du Client et du Tiers Archiveur.
Les liens peuvent être des liaisons spécialisées ou des liaisons par internet. Le fonctionnement du lien jusqu'à la plateforme d'archivage est sous la responsabilité du Client.

5.3.3 Evaluation de la qualité perçue par le client

La mesure de la qualité perçue par le Client est faite au travers des mesures effectuées par l'entreprise. Le [SMQ] de l'entreprise précise les modalités de mesure de qualité perçues dans le processus CSAT. Le Tiers Archiveur analyse les résultats de ces retours et met en place les plans d'actions quand cela est nécessaire.

6 Principes techniques

6.1 Identification des acteurs

La politique d'archivage définit les rôles suivants, les responsabilités de chacun sont décrites dans les sections suivantes du document :

- le Client ;
- le Tiers Archiveur (TA) ;
- l'Autorité d'Archivage (AA) ;
- le Service Producteur (SP) ;
- le Service Versant (SV) ;
- le Service de Contrôle (SC).

6.1.1 Le Tiers Archiveur (TA)

6.1.1.1 Responsabilité liée à la PA

Le TA est responsable de la rédaction, la mise à jour et de la diffusion de la PA de WL e-archiving. La présente PA, référencée par le contrat, définit les engagements des entités concernées pour la délivrance du Service d'Archivage Electronique fourni par WL e-archiving.

Les engagements que prend le Tiers Archiveur vis-à-vis de son Client sont définis dans un contrat ou dans ses annexes (convention d'archivage). Devront être présents ou référencés:

- la description de service convenu avec le Client ;
- les engagements sur la qualité de service convenus avec le Client ;
- une annexe technique décrivant les interfaces du système ainsi que les méthodes d'accès au service ;
- une annexe financière détaillant les conditions financières de la fourniture du service.

6.1.1.2 Responsabilité du TA

Le TA est responsable des obligations qui lui incombent, en application de la PA:

- le TA identifie le Service Versant et le Service Producteur lors des opérations sur les Archives ;
- lors du versement d'une Archive, la responsabilité du TA est engagée vis-à-vis du Client dès qu'il a émis l'accusé de réception fonctionnel de l'Archive versée ;
- le TA doit conserver l'intégralité des documents transmis par le Client ;
- le TA ne fait pas de conversion de format ;
- disposer d'une capacité de stockage suffisante et évolutive pour pouvoir assurer de façon continue la prise en charge des documents, en accord avec les engagements contractuels ;

- respecter les exigences minimales de la norme NF Z42-013, notamment les obligations du TA pour la gestion de la documentation (NF Z42-013 chapitre 12.1.4 Maîtrise de la documentation pour les audits) ;
- permettre un accès direct sécurisé pour consultation ou extraction des paquets d'informations archivés ;
- respecter l'application de la politique d'accès aux Archives définie par la Convention d'Archivage, notamment, prendre toute mesure technique pour garantir que les paquets d'informations archivés ne soient accessibles qu'aux personnes habilitées ;
- effectuer les destructions des Archives sous le contrôle du Client et, après exécution, lui fournir les attestations correspondantes ;
- garantir la confidentialité des documents qui lui sont confiées ou dont il peut avoir eu connaissance à l'occasion de la relation contractuelle avec son Client ;
- ne pas analyser et retraiter les documents confiées par le Client, sauf pour des travaux explicitement commandés par celui-ci (conversion de format par exemple) ;
- informer à l'avance le Client des modifications techniques devant intervenir sur ses systèmes et des conséquences sur la disponibilité ou sur le mode d'échange et de conservation des documents confiées ;
- en cas de reprise des Archives confiées par le Client, prendre toutes dispositions pour garantir à celui-ci, la restitution de l'intégralité des Archives et de l'ensemble des documents y afférant (journaux de cycle de vie par exemple) qui lui sont confiées en garantissant leur intégrité ;
- en fin de contrat ou en cas de cessation d'activité, se mettre en mesure de restituer intégralement au Client les paquets d'informations archivés et les éléments associés. Le TA s'interdit d'en conserver une copie ;
- maintenir la qualité des services prévus au contrat et précisés dans la Convention de services.

Il est à noter que les engagements suivants sont hors du périmètre de WL e-archiving et de la présente Politique :

- obtenir et maintenir les agréments nécessaires à l'hébergement d'Archives publiques. Néanmoins, le Tiers Archiveur pourra fournir à une organisation souhaitant réaliser l'archivage d'Archives publiques les moyens nécessaires à l'obtention des agréments nécessaires.

6.1.2 L'Autorité d'Archivage (AA)

L'AA est responsable de la définition de la Convention d'Archivage. Celle-ci définit, entre autre, le format des Archives acceptées ainsi que la politique d'accès aux Archives.
Pour préciser les conditions techniques mises en œuvre, le Service versant et l'Autorité d'archivage doivent passer un accord (convention, charte d'archivage,…) relative aux versements, aux traitements et aux accès des Archives. Cet accord doit être totalement conforme à la PA.

6.1.3 Le Client

Le Service d'Archivage est généralement un élément d'un Système d'Information plus large. Il est de la responsabilité du Client de s'assurer que le Service d'Archivage correspond à ses besoins et à ses contraintes réglementaires.
Le Tiers Archiveur fournit un ensemble d'éléments permettant au Client de facilité l'intégration du Service d'Archivage dans son Système d'Information.

6.1.3.1 Format des documents

Le Tiers Archiveur assure l'intégrité du document durant l'ensemble du cycle de vie (se référer au chapitre 3.1.6 du présent document), et s'engage à ne pas analyser le contenu des documents archivés. Par conséquent, le Tiers Archiveur ne peut garantir à lui seul la pérennité dans le temps du contenu informationnel du document.
Le Client est responsable du choix des formats d'archivage qui seront utilisés. Toutefois le Tiers Archiveur propose un ensemble de règles afin d'assurer une meilleure pérennité :

- il est conseillé au client d'utiliser des formats ouverts, c'est-à-dire des formats dont les spécifications sont facilement accessibles ;
- les formats reposant sur des normes locales ou internationales peuvent également être envisagés ;
- dans le cas d'un format propriétaire, le client doit s'assurer que ce format est largement répandu et que sa durée de vie est compatible avec la durée de vie des Archives. Les formats de présentation ainsi que les flux d'impression sont considérés comme des formats propriétaires ;
- dans le cas d'un format balisé, s'il fait référence à des ressources externes (DTD, XSD, feuille de style …), il est de la responsabilité du client d'archiver ces ressources et de les associer aux archives contenant des documents au format balisé. Lors de la communication, il est de la responsabilité du client de récupérer l'ensemble des documents nécessaires.

Les éléments suivants peuvent également aider dans le choix des formats cibles :

- limiter l'utilisation de format nécessitant une licence spécifique ;
- s'assurer que plusieurs solutions logicielles permettent d'accéder au contenu des documents ;
- vérifier qu'une solution logicielle open source permet d'accéder au contenu du document ;
- n'utiliser que des formats stables, c'est-à-dire sans mises à jour trop fréquentes.

Quand le choix est fait d'archiver des documents numériques dont le format n'est pas connu, la gestion de la perenité des documents est de la responsabilité du client.

En cas d'obsolescence de format de document archivé, Le Client est à l'initiative des choix d'évolutions de ces formats. Le Tiers Archiveur peut accompagner le Client dans cette demarche.

Les formats de presentation ne sont pas gérés par le service WL e-archiving, il est de la responsabilité du client de s'assurer de leur lisibilité dans le temps. Le Tiers Archiveur peut accompagner le Client dans cette demarche.

Le Tiers Archiveur accepte tout les formats de document, avec les réserves exprimées ci-dessus. La liste des formats pour un client donné sera précisée dans la convention de service.

6.1.3.2 Politique d'Archivage

Pour son propre usage, le Client doit définir une Politique d'Archivage. Ce document décrira les éléments nécessaires à la compréhension de l'intégration du Service d'Archivage dans le Système d'Information du Client.
Devront y figurer :

- une description des processus faisant intervenir le Service d'Archivage ;
- une description des documents à archiver ainsi que les métadonnées associées ;
- un plan de classement des Archives ;
- une description du cycle de vie de chaque type d'Archive ;
- une Politique de Sécurité de l'Information [PSI] décrivant les moyens de sécurisation des échanges ;
- une étude de plan capacitaire.

Ce document est la seule propriété du Client et ne devra pas obligatoirement être fourni au Tiers Archiveur. Il sera néanmoins utile lors de la création de la Convention d'Archivage entre le Client et le Tiers Archiveur.

6.1.3.3 Convention d'Archivage

La Convention d'Archivage est un document décrivant l'utilisation du Service d'Archivage par le Client. Il rassemble l'ensemble des informations de la Politique d'Archivage du Client permettant la mise en place du service par le Tiers Archiveur.

6.1.3.4 Versement

Lors du versement, il est de la responsabilité du Client de s'assurer de la qualité des documents fournis et des métadonnées transmises. Il doit s'assurer que ses dépôts sont conformes à la Convention d'Archivage.

6.1.3.5 Vérification des Accusés de Réception

Le Client doit contrôler le contenu de l'accusé de réception technique afin de s'assurer que la demande de dépôt a bien été effectuée, et l'accusé de réception fonctionnel afin de vérifier que la sécurisation de l'Archive est bien complète.
L'engagement du Tiers Archiveur ne tient qu'après émission d'un avis de réception technique positif lors du dépôt d'une Archive.

6.1.3.6 Protection des données personnelles

Au sens défini par le règlement européen concernant la protection des données personnelles [RGPD], le client est considéré comme responsable de traitement et doit s'assurer du respect dudit règlement par les différents acteurs ayant accès aux données personnelles.
Le Tiers Archiveur pourra conseiller le Client lors de la mise en place du projet d'archivage. WL e-archiving dispose des interfaces permettant la mise en conformité des documents si des données personnelles y sont stockées et si cela était nécessaire.

6.1.4 Le Service producteur (SP)

Le Service Producteur désigne l'entité fournissant les documents à archiver (documents et métadonnées). Il est hors du cadre de cette politique d'archivage.
Les responsabilités de sécurisation des documents sources sont portées par le SV qui peut, suivant l'organisation et le contexte projet, les déléguer au SP.

6.1.5 Le Service versant (SV)

Le Service Versant désigne l'entité qui transfère un document à verser à une Autorité d'Archivage.
Le Service Versant est responsable de la création des requêtes de dépose d'Archive sur le Service d'Archivage. Il doit s'assurer de la validité des requêtes d'archivage et de la validité des résultats reçus. Le Service Versant s'engage à fournir toutes les informations relatives à la nature et à la durée de vie de l'Archive ainsi que leur éventuel caractère confidentiel et les limitations d'accès à l'Archive concernée, le cas échéant.

Le SV peut s'assurer de la sécurisation de l'Archive au travers de la récupération de l'attestation fonctionnelle.
Il appartient au Service Versant de vérifier le caractère communicable de l'Archive ou du document d'Archives conformément à la législation et à la réglementation applicables en la matière (notamment la loi du 17 juillet 1978 modifiée et le Code du patrimoine).
Le Service Versant garantit que les supports et les Archives qu'ils contiennent sont en parfait état et exempts de tout virus ou autre dysfonctionnement susceptible d'avoir un impact sur la bonne exécution de la Politique d'Archivage et notamment sur les obligations de l'Autorité d'Archivage ou sur les moyens informatiques utilisés.

6.1.6 Le Service de Contrôle

Les Contrôleurs sont tenus d'exercer leurs contrôles dans le respect des textes législatifs et réglementaires qui encadrent leurs compétences. Il leur appartient, dès lors qu'ils relèveraient des difficultés pour exercer leurs contrôles, d'en avertir par tout moyen l'Autorité d'Archivage compétente afin qu'elle y remédie.

6.1.7 Les Utilisateurs et Usagers

Les Utilisateurs et les Usagers doivent respecter les conditions de consultation et de communication afférentes au Service d'Archivage Electronique et aux documents d'Archives traités.
Ils doivent également respecter la confidentialité, le cas échéant, des documents d'Archives traités et ne pas tenter d'y accéder s'ils ne disposent pas des droits associés.
Dans la mesure où l'Utilisateur ou l'Usager dispose d'un mode d'accès spécifique et personnel (authentification par identifiant / mot de passe), il s'engage à le conserver confidentiel et en faire un usage sous son contrôle exclusif.
De même, les Utilisateurs et les Usagers ne doivent pas tenter de détériorer tout ou partie du Service d'Archivage Electronique sécurisé et/ou de son contenu.

6.1.8 Les opérateurs

Les opérateurs sont les utilisateurs de la plateforme d'archivage, membre de l'organisation du Tiers Archiveur dont les activités visent au bon fonctionnement du système d'archivage.
Les rôles et les responsabilités des acteurs sont définis dans la Politique Générale [PG] en conformité avec la politique définie dans le Système de Management de la Qualité de l'entreprise [SMQ].

6.2 Organisation de la sécurité des systèmes d'information

Le Comité Mediacert Tiers Archiveur, dispose d'une Politique de Sécurité Opérationnelle pour ledit service. Cette politique est compatible avec la [PSI] de Worldline et étend la [PG] du TSP. Ces politiques sont chacune maintenues et revues régulièrement par leur entité responsable.
La Politique de Sécurité Opérationnelle est un document classifié à usage interne.
Une analyse de risque [AR] spécifique au Service d'Archivage a été menée et est régulièrement mise à jour. Un plan d'action issue de l'application de la [PSO] et de l'[AR] est maintenu à jour et vérifié régulièrement par le Comité Mediacert.
La composition et le mode de fonctionnement du Comité Mediacert sont définis dans la Politique Générale [PG].
Le Service d'Archivage dispose d'un Plan de Continuité de l'activité. Se référer au chapitre 5.1.2 Planification de la continuité de l'activité du présent document.

6.3 Contrôle d'accès

Les accès aux composants physiques de la plateforme sont strictement contrôlés en conformité avec la [PG] et la [PSI].
L'administration de la plateforme est strictement contrôlée. Seules des personnes identifiées et contrôlées ont accès aux moyens d'administration de la Plateforme.

6.4 Journalisation

Le Service d'Archivage met en place un ensemble de mesures afin de concentrer et d'analyser l'ensemble des événements de la plateforme (voir 4.2.2.4).

6.5 Scellement

Le scellement est réalisé par la signature de l'Empreinte du Fichier de Description de l'Archive. Cette signature est réalisée au moyen d'une clé privée certifiée par une autorité de certification reconnue. Ce scellement repose sur l'utilisation de format standard.

6.6 Horodatage

Une contremarque de temps est présente dans le scellement de l'Archive. Cette contremarque de temps émane d'une source de temps fiable.

6.7 Utilisation de disques réinscriptibles

Les Archives sont stockées sur des disques durs magnétiques, soit des disques réinscriptibles. Ce support est conforme aux recommandations actuelles par l'usage de moyen cryptographique pour le scellement, le chiffrement et la vérification régulière de l'état du fond d'Archive.