

CADRE D'INTEROPÉRABILITÉ

Unité de Gouvernance Digitale - UGD

<https://digital.gov.mg>

Etat	Version	Date de la version
Validé	1.0.0	Août 2022

VERSIONS DU DOCUMENT

Version	Date	Auteur / Fonction : Nom	Objet de la mise à jour
0.1	Déc 2021	AMOA/PO/Architectes SI	Création
0.2	Mar 2022	AMOA/PO/Architectes SI	Amélioration continue
0.3	Mar 2022	AMOA/PO/Architectes SI	Intégration retour WB
0.4	Jui 2022	AMOA/PO/Architectes SI	Intégration des remarques venant de toutes les parties prenantes suite aux différents ateliers
0.5	Aoû 2022	AMOA/PO/Architectes SI	Intégration des mises à jour après benchmark et compilation des retours des PMOS
1.0.0	Sep 2022	AMOA/PO/Architectes SI	Intégration des retours remontés lors de l'atelier d'interopérabilité à Fianarantsoa du 23 aout 2022
1.0.1	Oct 2022	AMOA/PO/Architectes SI	Intégration des retours de nos partenaires
1.0.2	Nov 2022	AMOA/PO/Architectes SI	Revue pour publication de la version officielle

DESTINATAIRES DU DOCUMENT

Diffusion pour action	Tous les services publics
Diffusion pour information	Secteur privé

VALIDATION DU DOCUMENT

Version	Valideur 1 Fonction : Nom	Date	Valideur 2 Fonction : Nom	Date
V.1.0.2	Jean Luc RAZAFINDRAMINTSA CDO Pi	10/11/22	Helijao RAKOTOMANGA Architecte	10/11/22

DOCUMENTS DE RÉFÉRENCE

N°	Classement	Titre
1		Manuel et standards de services
2		Norme et standard de l'interopérabilité
3		

LISTE DES ABREVIATIONS

A2A : Administration to Administration

A2B : Administration to Business

A2C : Administration to Customer

API : Application Programming Interface

CA : Certificate Authority (autorité de certification)

CIRT : Computer Incident Response Team

CMIL : Commission Malagasy de l'Informatique et des Libertés

CNI : Comité National d'Interopérabilité

CNaPS : Caisse Nationale de Prévoyance Sociale

CSI : Comité Sectoriel d'Interopérabilité

DGI : Direction Générale des Impôts

EDBM : Economic Development Board of Madagascar

HTTPS : HyperText Transfer Protocol Secure

ID : Identification

INSTAT : Institut National de la Statistique

JSON : JavaScript Object Notation

MEF : Ministère de l'Economie et des Finances

MEN : Ministère de l'Education Nationale

MID : Ministère de l'Intérieur et de la Décentralisation

MINJUS : Ministère de la Justice

MINSanP : Ministère de la Santé Publique

MNDPT : Ministère du développement Numérique, de la transformation Digitale, des Postes et des Télécommunications

OCSP : Online Certificate Status Protocol

SI : Système d'Informations

SSL : Secure Sockets Layer

SSO : Single Sign-On

UGD : Unité de Gouvernance Digitale

XML : eXtensible Markup Language

X-ROAD SS : X-ROAD Security Server

TABLE DES MATIÈRES

I. GENERALITES	6
1.1 Contexte et objectifs	6
1.1.1 Contexte générale	6
1.1.2 Objectifs	6
1.1.3 Principes de la démarche entreprise	7
1.1.4 Résultat attendu	7
1.1.5 Elaborations et mise à jour du cadre d'interopérabilité	8
1.1.5.1 Elaboration	8
1.1.5.2 Mise à jour	8
1.2 Définitions	8
1.2.1. Interopérabilité	8
1.2.2 Cadre d'Interopérabilité	9
1.3 Champs d'application du cadre d'interopérabilité	9
1.4 Bénéfices	9
II. CADRE D'INTEROPÉRABILITÉ	10
2.1 Principes fondamentaux d'interopérabilité	10
2.2 Niveaux d'interopérabilité	12
2.2.1 Interopérabilité juridique	12
2.2.2 Interopérabilité organisationnelle	13
2.2.3 Interopérabilité sémantique	13
2.2.4 Interopérabilité technique	14
2.3 Protocole d'interopérabilité	15
2.4 Gouvernance des données et le "Once Only Principle"	15
2.4.1 Gouvernance de données	15
2.4.2 Once only principle	16
2.5 Modèle organisationnel	17
2.5.1 Autorité de gouvernance	17

2.5.2 Comité National d'InterOPérabilité (CNIOP)	17
2.5.3 Comités Sectoriels pour l'Interopérabilité (CSIOP)	18
2.5.4 Entités Membres	18
2.5.5 Le prestataire de services de confiance	19
2.5.6 Autorité de certification	20
2.5.7 Autorité d'horodatage	21
2.6 Catalogue des services d'interopérabilité	21
2.7 Architecture	21
2.8 Technologie	23
III. DIRECTIVES ET RÈGLES OPÉRATIONNELLES	24
3.1 Evaluation de la préparation à l'interopérabilité	24
3.2 Approche Orientée Service	25
3.3 Conformité de l'interopérabilité entre entités	25
3.4 Outils pour la mise en œuvre de l'interopérabilité	25
3.4.1 Cartographie du Système d'information	25
3.4.2 Modèle d'interopérabilité	25
IV. DIRECTIVES À SUIVRE	26
4.1 Transparence	26
4.2 Réutilisabilité	26
4.3 Centré sur l'utilisateur	27
4.5 Sécurité, confidentialité et intégrité	27
4.6 Neutralité technologique et portabilité des données	27
4.7 Simplification administrative	27
4.9 Évaluation de l'efficacité et de l'efficience	27
Références	28

I. GENERALITES

1.1 Contexte et objectifs

1.1.1 Contexte générale

Depuis l'émergence de la transformation digitale à l'échelle mondiale, plusieurs aspects des organisations se retrouvent actuellement contraints à suivre le mouvement notamment l'aspect social, humain et économique. De plus en plus de pays se ruent actuellement vers la digitalisation de leurs services¹ publics dans le but de gagner du temps, de l'argent et plus d'efficacité.

De ce fait, le gouvernement malagasy, par l'intermédiaire de l'e-Gouvernance², a élaboré une stratégie pour améliorer la gestion des recettes et l'accès aux services publics pour les particuliers et les entreprises. En effet, il s'est engagé à asseoir une Administration de proximité efficace au service de la population. Il s'agit d'une stratégie politique qui sera transformée en stratégie digitale.

L'Unité de Gouvernance Digitale a donc été mise en place au sein de la Présidence de la République, suivant les objectifs principaux, pour appuyer les institutions malagasy dans tous les projets qui feront l'objet de digitalisation.

1.1.2 Objectifs

L'objectif principal du présent cadre est de mettre en place les aspects techniques et organisationnels de l'interopérabilité afin de proposer de meilleurs services publics répondant aux besoins des citoyens à savoir :

- Améliorer la gouvernance du domaine via la création d'organes officiels dédiés, la définition plus claire et la formalisation des rôles respectifs ainsi qu'une plus forte implication et responsabilisation de tous les acteurs concernés au niveau national ;
- Intensifier et étendre la collaboration entre les différents acteurs ou secteurs concernés ;
- Améliorer l'échange d'informations entre les différentes structures de l'administration publique pour satisfaire aux exigences légales ou aux engagements politiques ;
- Développer et systématiser la communication dans le domaine, notamment via la création d'un catalogue de produits d'interopérabilité défini sur la base de la cartographie à établir ;

¹ ITIL entend par service « l'ensemble des moyens mis en œuvre pour produire de la valeur pour un client, sans que celui-ci n'en supporte ni les coûts spécifiques et supplémentaires ni les risques associés »

² L'e-Gouvernance ou la gouvernance électronique est l'application des Technologies de l'Information et de la Communication pour la fourniture de services gouvernementaux, l'échange d'informations, les transactions de communication, l'intégration de divers systèmes et services autonomes entre gouvernements et citoyens, Gouvernement et entreprises, gouvernement et gouvernement, et gouvernement et employés, ainsi que les processus et interactions de back-office dans l'ensemble du cadre de travail gouvernemental.

- Généraliser et systématiser une approche qui, dès le départ, met l'interopérabilité au centre de chaque projet et de toute action ou décision concernée (**Interoperability by design**) : cela signifie notamment que des procédures spécifiques à l'interopérabilité doivent être intégrées de manière systématique dans les processus de gestion de projet, d'assurance qualité, de suivi et de contrôle qui sont à appliquer dans le cadre de la mise en place ou de la gestion des services ;
- Pérenniser les systèmes d'information publics grâce à l'emploi de normes et standards reconnus;
- Faire en sorte que les principes de ce cadre devienne une référence aux exigences nécessaires à la fourniture de services publics à prendre en compte et à suivre par tous les organismes concernés.

1.1.3 Principes de la démarche entreprise

L'objectif principal du présent cadre est de mettre en place les aspects techniques et organisationnels de l'interopérabilité afin de proposer de meilleurs services publics répondant aux besoins des citoyens à savoir :

- L'approche adoptée pour l'élaboration du cadre d'interopérabilité repose sur les principes suivants :
 - Appropriation des expériences issues de la démarche d'interopérabilité réalisée :
 - La réalisation d'une phase expérimentale (POC³) qui a permis d'identifier la base technologique d'un futur écosystème d'interopérabilité;
 - La mise en place du premier écosystème interopérable avec le projet Orinasa⁴ qui a permis l'échange de données sécurisé entre EDBM, DGI, MINJUS et INSTAT;
 - Le démarrage de la démarche nationale d'interopérabilité.
- Inclusion des parties prenantes de l'Etat Malagasy :
 - La constitution d'un task force des institutions en première ligne sur les projets d'interopérabilité avec l'UGD;
 - L'élaboration du document transcrivant les exigences et les besoins en interopérabilité de l'Etat Malagasy;
 - L'adoption du document par les parties prenantes issus des travaux communs.

1.1.4 Résultat attendu

Le résultat à court terme est d'avoir, dans un premier temps, un **Cadre d'Interopérabilité** qui va

³ Une preuve de concept (en l'anglais proof of concept, POC) est une réalisation ayant pour vocation de montrer la faisabilité d'un procédé ou d'une innovation.

⁴ "Orinasa" est un espace dédié aux porteurs de projets et entrepreneurs ayant pour objectif d'informer, préparer et orienter dans le processus de création d'entreprise (<https://orinasa.edbm.mg>).

aider au renforcement de la vision d'unité de l'État.

Ce cadre va donc contribuer à l'amélioration de la communication, fournir et permettre l'utilisation des services d'administration numériques efficaces pour améliorer la qualité de vie des citoyens.

A terme, le Cadre d'Interopérabilité sera le document qui va accompagner les entités dans le développement de leurs capacités à échanger des informations, indépendamment des restrictions ou de leur taille .

Par ailleurs, assurer une sécurité et instaurer la confiance entre les institutions de l'écosystème interopérable fait également partie des résultats attendus. Les éléments qui les permettent seront vus dans ce document cadre.

1.1.5 Elaborations et mise à jour du cadre d'interopérabilité

1.1.5.1 Elaboration

La présente version du cadre d'interopérabilité a été élaborée par les parties prenantes sur la base de l'analyse de l'existant et des besoins en interopérabilité des administrations publiques (échange, sécurité et intégrité de données, capacité métier et technique, etc ...) quant aux principes de base, modèles et recommandations d'interopérabilité.

Elle s'applique donc à toute réalisation de projets d'interopérabilité au sein de l'administration publique malgache et prend en compte les commentaires des acteurs publics.

Cette dernière est la première version officielle à Madagascar. Les parties prenantes sont donc tenues de suivre et d'appliquer les recommandations qui y sont contenues.

1.1.5.2 Mise à jour

Le cadre d'interopérabilité doit faire objet de mise à jour régulière et doit s'adapter aux évolutions technologiques ainsi qu'aux besoins d'interopérabilité des administrations publiques.

1.2 Définitions

Avant de rentrer dans le vif du sujet, il serait judicieux de citer quelques définitions importantes.

1.2.1. Interopérabilité

L'interopérabilité désigne la capacité d'un objet ou d'un système à communiquer et à fonctionner avec d'autres objets ou d'autres systèmes existants ou futurs, sans restriction d'accès ou de mise en œuvre, et de se comprendre mutuellement ainsi que de fonctionner en synergie. Il constitue donc un ensemble de règles, basées sur des normes et standards, permettant aux administrations publiques et aux institutions privées de partager des informations entre eux ainsi qu'à des usagers externes pour intégrer ces dernières au sein de processus métiers dématérialisés.

L'interopérabilité est rendue possible grâce à :

1. La conformité commune à un ensemble de normes et standards génériques;
2. La conformité à un ensemble de conventions architecturales;
3. Une conception architecturale modulaire qui définit le cadre dans lequel s'applique ces normes, standards et conventions.

Il est important de souligner que ces trois éléments sont nécessaires et indissociables. En effet, même si les deux premiers éléments sont en place, l'absence du troisième rendra très difficile l'intégration des applications informatiques car leurs fonctionnalités ne seront pas complémentaires.

1.2.2 Cadre d'Interopérabilité

Le cadre d'interopérabilité définit l'ensemble des principes, des recommandations et des lignes directrices qui guident les efforts politiques, les entités juridiques, organisationnelles, sémantiques, syntaxiques et techniques, afin de faciliter l'échange sûr et efficace d'informations.

Le cadre d'interopérabilité est destiné à améliorer la coopération au sein de l'État et entre l'État et ses partenaires. Le cadre d'interopérabilité sert de guide et de référentiel pratique à toute entité (publique, privée ou les organismes non gouvernementaux) ayant des besoins d'interopérabilité.

1.3 Champs d'application du cadre d'interopérabilité

Le champ d'application du cadre d'interopérabilité couvre trois types d'interactions :

- **A2A (administration à administration)**, qui fait référence aux interactions entre les structures de l'administration publique ;
- **A2B (administration à entreprise)**, qui fait référence aux interactions entre les structures de l'administration publique et les entreprises ;
- **A2C (administration aux citoyens)**, qui fait référence aux interactions entre les structures de l'administration publique et les citoyens.

1.4 Bénéfices

Les bénéfices qui devraient découler de ce cadre sont :

- Des systèmes d'information plus efficaces et plus efficaces ;
- Une vision plus complète et plus globale des initiatives et activités existantes liées à l'interopérabilité et à l'administration électronique ;
- Une gouvernance nationale commune et coordonnée de l'interopérabilité ;

- Un cadre d'interopérabilité qui facilite et accélère le progrès en matière d'interopérabilité en général et le partage, la réutilisation et le développement en commun des services en particulier ;
- Plus de transparence et d'ouverture en ce qui concerne à la fois l'information sur l'existence des services et la conception de ces derniers, et les données détenues par les acteurs concernés dans une optique de réutilisabilité et de respect des normes légales applicables.

II. CADRE D'INTEROPÉRABILITÉ

2.1 Principes fondamentaux d'interopérabilité

Les parties prenantes de l'interopérabilité (administrations publiques, institutions privées, etc.) devraient appliquer les principes fondamentaux qui suivent :

Principe 1 : Transparence

Les administrations publiques, les citoyens et les entreprises peuvent visualiser et comprendre les règles administratives, les processus, les données, les services et la prise de décision dans les systèmes.

Principe 2 : Réutilisabilité

Les administrations publiques ayant des besoins particuliers se réfèrent aux solutions déjà existantes, qui ont fait preuve d'efficacité ailleurs.

Cela nécessite que l'administration publique soit ouverte au partage et à l'interopérabilité des cadres de confiance et des solutions, concepts, cadres, spécifications, outils et composants avec d'autres.

Principe 3 : Centré sur l'utilisateur

Les besoins des utilisateurs priment lors de la détermination des services publics à fournir et de la manière dont ces derniers doivent être fournis. Par conséquent, les besoins et les exigences des utilisateurs guident la conception et le développement des services publics conformément aux attentes suivantes :

- Une approche de prestation de services multicanale (disponibilité de canaux alternatifs, physiques et numériques, pour accéder à un service), qui est un élément important de la conception du service public, car les canaux utilisés par les utilisateurs peuvent différer selon les situations qui se présentent à eux et leurs besoins.
- La nécessité de mettre un point de contact unique à la disposition des usagers, pour masquer la complexité administrative interne et faciliter l'accès aux services publics.
- Le recueil systématique des commentaires des utilisateurs, qui devront être évalués et utilisés pour concevoir de nouveaux services publics et améliorer ceux qui existent déjà.

Principe 4 : Sécurité, confidentialité et intégrité

Les citoyens et les entreprises doivent avoir la certitude que lorsqu'ils interagissent avec les autorités publiques, ils le font dans un environnement sûr, digne de confiance et dans le respect total des normes et réglementations applicables. Cela traduit la disponibilité, la confidentialité, l'authenticité, l'intégrité et la non-répudiation⁵ des informations fournies par les citoyens et les entreprises dans le but d'assurer la sécurité et la confidentialité de tout l'écosystème interopérable malagasy.

Chaque administration est également responsable de tout acte de la/des personne(s) qui détient(ent) les données d'accès liées à l'interopérabilité au sein de celle-ci.

Cela demande une vérification, voire une mise à jour systématique de toutes ces données d'accès. Il est important de responsabiliser le(s) point(s) focal(aux) de chaque entité sur l'importance des accès que l'on va lui/leur confier.

Principe 5 : Neutralité technologique et portabilité des données

Les administrations publiques doivent se concentrer sur les besoins fonctionnels et minimiser les dépendances technologiques, pour éviter d'imposer des limitations techniques spécifiques et rester agiles pour s'adapter à l'environnement technologique en évolution rapide.

Les administrations publiques devraient permettre l'accès et la réutilisation de leurs services publics et de leurs données, quelles que soient les technologies ou produits spécifiques.

Les données doivent impérativement être réutilisables dans différents systèmes.

Principe 6 : Simplification administrative

Les processus administratifs doivent être rationalisés et améliorés pour qu'ils offrent de la valeur publique. La mise en œuvre de systèmes devrait être soutenue par des moyens électroniques, de même pour leurs interactions avec d'autres administrations publiques, citoyens et entreprises. La numérisation des services publics devrait se dérouler selon les concepts suivants :

- Numérique par défaut, le cas échéant, afin qu'il y ait au moins un canal numérique disponible pour accéder et utiliser un service public donné.
- Numérique d'abord, ce qui signifie que la priorité est donnée à l'utilisation des services publics via les canaux numériques tout en appliquant le concept de livraison multicanale, comme la coexistence de canaux physiques et numériques.

Principe 7 : Évaluation de l'efficacité et de l'efficience

Pour évaluer l'efficacité et l'efficience de l'interopérabilité, il faut principalement considérer : le retour sur investissement, le coût total de possession, le niveau de flexibilité et d'adaptabilité, la charge administrative réduite, la réduction des risques, la transparence, la simplification,

⁵ La non-répudiation est l'une des propriétés de l'information considérées en cybersécurité (avec la confidentialité, l'intégrité et la disponibilité). Elle consiste en l'assurance qu'une action sur la donnée réalisée au nom d'un utilisateur (après authentification) ne saurait être répudiée par ce dernier. Tout comme la confidentialité et l'intégrité, la non-répudiation s'appuie sur des mécanismes de chiffrement.

l'amélioration du fonctionnement méthodes ainsi que le niveau de satisfaction et les impacts sur les utilisateurs.

2.2 Niveaux d'interopérabilité

Un échange réussi entre parties prenantes nécessite la prise en compte de différentes problématiques qui peuvent se décomposer en « niveaux d'interopérabilité ».

Les tableaux ci-après présentent quatre niveaux d'interopérabilité : **juridique**, **organisationnel**, **sémantique** et **technique**.

À chaque niveau correspondent des standards et des principes sur lesquels les parties doivent s'aligner pour concevoir et opérer des échanges efficacement.

2.2.1 Interopérabilité juridique

Objectif général	S'assurer que les organisations opérant sous différents cadres juridiques, politiques et stratégies peuvent travailler ensemble
Buts	<ol style="list-style-type: none"> 1. Appliquer les lignes directrices sur l'adéquation réglementaire de la loi sur les procédures administratives; 2. Identifier les lacunes, les différences et les obstacles juridiques à la création de services publics intégrés; 3. Créer des réglementations qui facilitent l'enregistrement centralisé des informations; 4. Définir les compétences pour la gestion des enregistrements primaires; 5. Définir des réglementations pour l'accès et la protection des données.

Il faut savoir que chaque administration publique, qui fournit un service public, œuvre dans un cadre juridique propre à elle-même. L'interopérabilité juridique consiste donc à garantir que les organisations fonctionnant sous différents cadres juridiques, politiques et stratégiques malagasy puissent fonctionner ensemble.

Par conséquent, un soutien politique est indispensable :

- Dans les cas où de nouveaux services ne sont pas directement liés à un instrument législatif, mais sont créés afin de fournir des services publics de meilleure qualité qui est plus centré sur l'utilisateur;
- Aux engagements communs d'interopérabilité, mis en œuvre dans le but d'optimiser la coopération entre administrations publiques. Ceci ne sera efficace que si les parties

prenantes partagent la même vision, s'accordent sur des objectifs communs et harmonisent leurs priorités.

Il est important d'effectuer des contrôles d'interopérabilité par le biais de l'analyse de la législation en vigueur pour mettre en évidence les obstacles à l'interopérabilité que l'on veut mettre en place.

2.2.2 Interopérabilité organisationnelle

Objectif général	Aligner les processus métiers, les responsabilités et les attentes qui permettent la mise en œuvre de services intégrés.
Buts	<p>Évaluer et appliquer les lignes directrices de l'architecture des services numériques, ce qui comprend:</p> <ol style="list-style-type: none"> 1. Documenter les processus métier à l'aide de techniques de modélisation inclusivement adoptées. 2. Clarifier et officialiser les relations organisationnelles internes nécessaires à la mise en œuvre et au fonctionnement d'un service public. 3. Définir et formaliser les relations extérieures (fournisseur / consommateur) nécessaires à la mise en œuvre et au fonctionnement d'un service public.

L'interopérabilité organisationnelle est liée aux organisations et aux processus notamment mis en œuvre pour favoriser et opérer les échanges entre les entités de l'administration publique malagasy. Elle concerne aussi les compétences et les connaissances associées au fonctionnement de ces organisations.

2.2.3 Interopérabilité sémantique

Objectif général	Garantir que le format et la signification précise des données et informations échangées sont correctement interprétés, c'est-à-dire "que ce qui est transmis est ce qui est compris".
Buts	<ol style="list-style-type: none"> 1. Appliquer les directives de la politique nationale sur les données ouvertes pour générer, collecter, gérer, partager, protéger et conserver les données. 2. Donner la priorité à la gestion des métadonnées, des données de base et des données de référence en appliquant les normes et standards nationaux et sectoriels. 3. Former des communautés sectorielles et intersectorielles pour créer des normes d'information ouvertes.

L'interopérabilité sémantique détermine le niveau d'interopérabilité permettant aux entités qui participent au processus d'interopérabilité de se comprendre mutuellement. La sémantique recouvre à la fois la signification des mots, le rapport entre le sens des mots (homonymie, synonymie, etc.), mais aussi le cycle de vie d'une information. Comme toute collaboration entre entités nécessite une communication, au sens d'un échange d'informations, ces dernières s'entendent sur la signification des données qu'elles échangent et sur le contexte de cet échange. Il est question ici de concept métier (exemple : une entreprise, un chiffre d'affaires, un revenu fiscal de référence, etc.).

Trois éléments sont mis en évidence vis à vis d'un cadre d'interopérabilité entre plusieurs entités :

- **Les méthodes et les langages de spécification** : concerne la formalisation des échanges entre les parties prenantes.
- **La conception des échanges** : Il faut décrire les concepts de l'échange et mettre en œuvre une démarche générique permettant d'analyser les échanges. Concerne la description des de l'échange et la mise en œuvre d'une démarche générique permettant l'analyse de ces échanges.
- **Les ressources sémantiques pouvant être ré-utilisées** : Le recensement des ressources sémantiques susceptibles d'être utilisées lors de la conception des échanges est important.

2.2.4 Interopérabilité technique

Objectif général	Garantir la communication entre les systèmes d'information pour mettre en œuvre des services intégrés
Buts	<ol style="list-style-type: none"> 1. Appliquer les directives d'échange de données électroniques pour planifier les services de données. 2. Appliquer les directives d'interopérabilité technique pour développer des services de données. 3. Intégrez vos services dans la plateforme nationale d'échange de données . 4. Prioriser les solutions pour intégrer les informations et soutenir la prestation de services publics.

L'interopérabilité technique est structurée selon les domaines suivants :

- **Présentation et accès à l'information** : ce domaine traite des règles de navigation et de restitution de l'information.
- **Services web et intégration de données** : ce domaine traite des technologies d'échanges entre Systèmes d'Information.

- **Multimédia** : Le multimédia traite des technologies de communication entre humains, notamment de la messagerie et de la téléphonie.
- **Infrastructure** : ce domaine traite des technologies élémentaires nécessaires aux échanges, notamment des protocoles réseau.

2.3 Protocole d'interopérabilité

Le protocole détermine le schéma d'interopérabilité ainsi que les normes et standards à appliquer à chaque niveau d'interopérabilité. Par ailleurs, le protocole précise les mécanismes de validation des traitements entrant dans le cadre du processus d'interopérabilité ainsi que les ressources à engager pour exécuter de façon optimale le processus. Les acteurs qui interviennent dans la mise en place et l'exécution d'un processus d'interopérabilité s'approprient, alors, des indications prescrites dans le protocole correspondant au schéma d'interopérabilité concerné.

2.4 Gouvernance des données et le “Once Only Principle”

2.4.1 Gouvernance de données

Les données sont des éléments de la mise en œuvre et de l'instauration de la politique d'e-gouvernance. La gouvernance des données est la composante la plus importante de cette politique. Elle est la garante de la sécurité, de la cohérence et de la standardisation des données publiques. La gouvernance des données définit le flux de données à travers les organisations.

La gouvernance des données est basée sur les principes suivants :

- **La précision et l'exactitude** : les données doivent impérativement refléter la réalité, ce qui nécessite de déterminer leurs sources et de les valider ;
- **L'actualisation** : il est important de vérifier, de manière ponctuelle et régulière, que les informations stockées sont actualisées ;
- **La complétude** : les données collectées doivent être suffisamment complètes pour être analysées et exploitées ;
- **L'homogénéité, la cohérence et l'unicité** : les données hébergées dans les différents systèmes doivent refléter les mêmes informations et être synchronisées pour éviter les erreurs ou les doublons;

- **La validité** : il faut absolument faire attention à ce que les données respectent les normes et la réglementation future qui sera émise par l'autorité indépendante : la Commission malagasy sur l'informatique et les libertés (CMIL⁶);
- **L'opportunité** : il ne faut pas se contenter de collecter des données quelconques, mais de récupérer des informations essentielles à la prise de décision.

Au-delà de ces critères, les données de qualité doivent également répondre à un processus de récupération visant justement à éviter les informations dupliquées ou erronées. Il est donc essentiel pour le gouvernement de se doter de règles de gouvernance des données et de mettre en application le concept de sources autoritaires d'information gouvernementale.

Toutefois, il faut savoir que la collecte des données représente un coût, aussi bien pour le gouvernement, que pour l'entité qui la fournit. Il est donc nécessaire de l'optimiser afin de :

- Ne pas collecter les mêmes données plusieurs fois. Ce qui nous amène à mettre en commun les données entre les entités et choisir les données utiles au plus grand nombre, dans des formats pertinents;
- Ne pas multiplier la saisie. Ce qui nous amène à privilégier l'interconnexion avec les systèmes d'information existants au plus près de la source de référence. Le système d'information du gouvernement doit donc être accessible à toutes les parties prenantes via des interfaces standardisées.

Il est donc essentiel pour le gouvernement de se doter de règles de gouvernance des données et de mettre en application le concept de sources autoritaires d'information gouvernementale.

Ainsi, les administrations publiques ou institutions privées qui font partie de l'interopérabilité ne devraient avoir à fournir leurs services qu'une seule fois dans leurs échanges, c'est le "Once Only Principle".

2.4.2 Once only principle

"**Once only principle**" est le principe selon lequel les informations ne sont fournies aux consommateurs d'informations qu'une seule fois par la source propriétaire et qu'il n'existe aucune autre source d'informations pour les mêmes informations. Les entités doivent prendre des mesures pour partager des données entre eux, dans le respect des règles de confidentialité, d'intégrité et de protection des données.

L'objectif à long terme de l'interopérabilité de Madagascar est d'appliquer le "once only principle". Ceci est défini de manière différente selon chaque pays. Pour certains, il fait référence au stockage de données, ce qui signifie stocker les données collectées dans une seule base de données. Dans d'autres pays, la collecte de données est faite une seule fois et les données ne peuvent être

⁶ La Commission Malagasy de l'Informatique et des Libertés ou CMIL est l'autorité de contrôle en charge à Madagascar du respect des obligations en matière de données à caractère personnel.

transmises qu'une seule fois aux administrations publiques, mais plusieurs référentiels de données sont possibles. D'autres pays combinent les deux approches et exigent que les données ne soient collectées qu'une seule fois et stockées dans une seule base de données.

2.5 Modèle organisationnel

L'organisation du système d'interopérabilité de Madagascar est composé de :

- Une autorité de gouvernance (UGD);
- Un comité national d'interopérabilité;
- Un comité sectoriel d'interopérabilité dans chaque entité;
- Des entités membres (à la fois les fournisseurs et consommateurs de services);
- Un Service de confiance constitué par : une autorité de certification, une autorité de signature électronique et une autorité d'horodatage.

2.5.1 Autorité de gouvernance

L'UGD étant le centre de l'écosystème d'interopérabilité à Madagascar, elle assurera donc, au début, l'autorité de gouvernance ce qui lui confère la responsabilité de tous les aspects des opérations. Parmi lesdites "responsabilités" figurent : la définition des réglementations et des pratiques, l'acceptation de nouveaux membres, l'assistance aux membres et l'exploitation des composants centraux de l'écosystème d'interopérabilité.

Ainsi, les nouveaux membres qui souhaitent intégrer le système d'interopérabilité soumettent leurs demandes et signent les accords compte tenu des réglementations et normes imposées par l'autorité de gouvernance.

2.5.2 Comité National d'InterOPérabilité (CNIOP)

A terme, un **Comité National d'Interopérabilité** impliquant toutes les parties prenantes de l'interopérabilité à Madagascar devra être mis en place. La mission de CNIOP est de faire progresser l'interopérabilité de manière générale au niveau national et transsectoriel. Il chapeaute les Comités Sectoriels pour l'Interopérabilité (CSIOP), qui ont pour mission de faire progresser l'interopérabilité au niveau purement sectoriel. Les CSIOP se gèrent et s'organisent de façon autonome. Ce CNIOP aura pour rôle de définir la politique et la stratégie nationale d'interopérabilité. Il s'assurera aussi de régler les éventuels conflits entre les participants dans le cadre d'interopérabilité. Ainsi, le management de l'écosystème d'interopérabilité malagasy sera donc assuré par le CNIOP. Ceci, dans le but de faire respecter la normalisation ainsi que d'assurer une pérennité de l'écosystème.

Ci-dessous une première ébauche de l'organisation du comité d'interopérabilité :

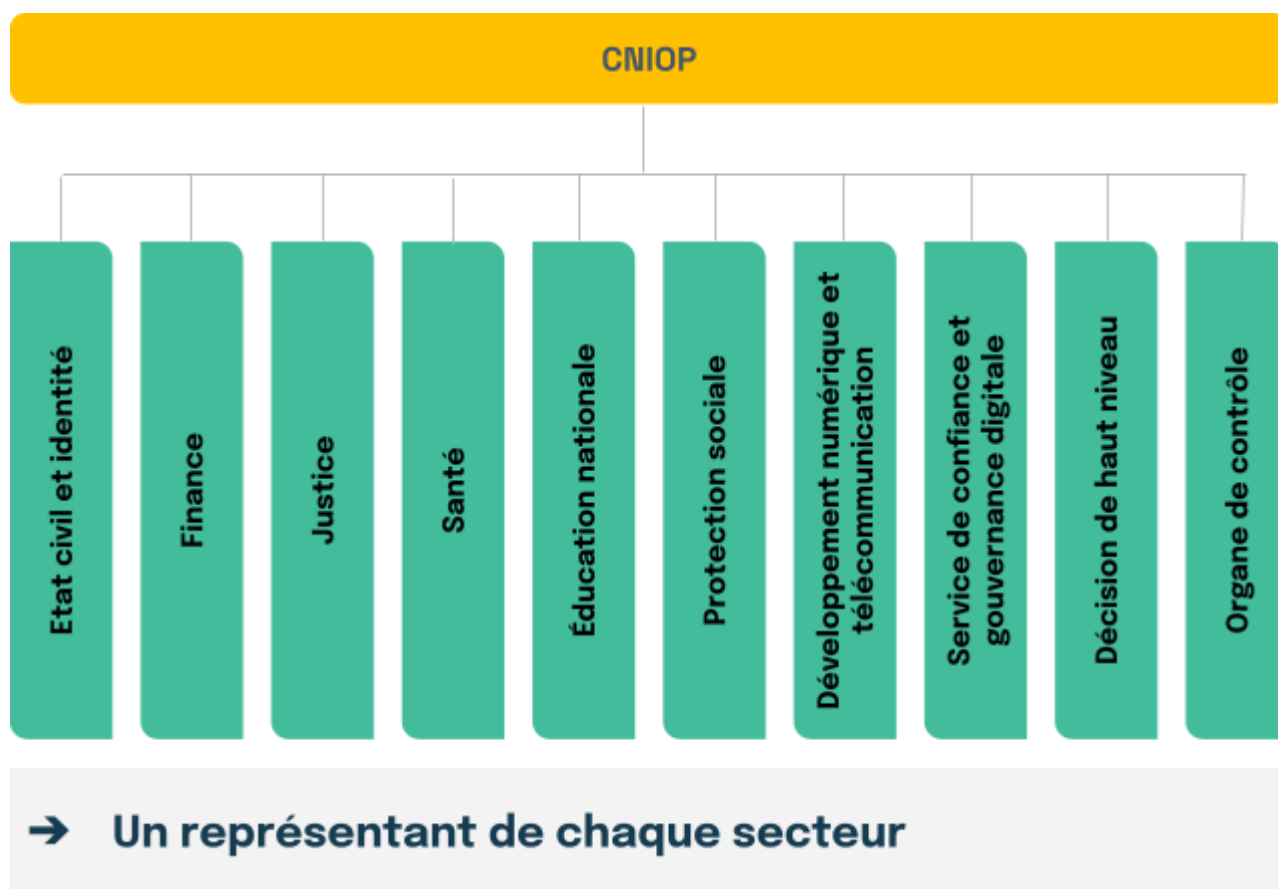


Figure 1 : Structure organisationnelle pour la gouvernance de l'interopérabilité

2.5.3 Comités Sectoriels pour l'Interopérabilité (CSIOP)

Les CSIOP ont pour mission de faire avancer l'interopérabilité au niveau purement sectoriel. Les CSIOP sont autonomes dans leur gestion et organisation. Ils se chargent de la stratégie du Système d'information au niveau sectoriel en coordination avec la direction des systèmes d'information de l'entité et le CNIOP.

2.5.4 Entités Membres

Les membres du système d'interopérabilité sont des organisations qui ont rejoint l'écosystème et qui produisent et/ou consomment des services avec d'autres membres. Une entité membre peut être un fournisseur de services, un consommateur de services ou les deux à la fois. Les organisations peuvent devenir membres d'un écosystème en suivant le processus d'intégration défini dans le cadre d'interopérabilité. De plus, les membres doivent avoir accès au composant technique nécessaire à l'échange de données.

Par ailleurs, un écosystème fonctionnel nécessite deux types de services de confiance : i) l'autorité d'horodatage et de signature et ii) l'autorité de certification. Le fournisseur de services de confiance

est une organisation ou unité de l'administration publique fournissant ces services. Les fournisseurs de services de confiance, ou les services peuvent également être fournis et maintenus par l'autorité de gouvernance.

2.5.5 Le prestataire de services de confiance

Les Services de Confiance permettent :

- La création, la vérification et la validation :
 - de l'Autorité de certification;
 - des signatures électroniques;
 - de l'horodatage;
 - des services de livraison électronique certifiée;
 - des certificats pour l'authentification des sites Internet.

- La préservation des signatures électroniques, des cachets ou certificats liés aux services de base.

Le prestataire de services de confiance est celui qui dispose de l'ensemble des moyens technologiques qui permettent de traiter les informations générées dans un format électronique. Il y applique des méthodes destinées à en assurer :

- la confidentialité;
- l'intégrité;
- l'authenticité;
- la traçabilité ou la preuve.

Ce prestataire met en place, auprès des parties prenantes de l'interopérabilité, des mécanismes d'identification et d'authentification électronique sécurisés (régis par le cadre légal en vigueur) afin d'assurer et de fluidifier les différents échanges de données et de services de base.

Pour garantir un niveau élevé et assuré de sécurité lors de l'échange d'informations, plusieurs mécanismes d'identification et d'authentification électronique des fournisseurs et consommateurs de services sont appliqués, à savoir : la signature électronique, l'horodatage électronique ou l'application de cachets électroniques. L'application de ces mécanismes permet de mettre en place des procédures d'archivage à long terme et sécurisées.

Plusieurs avantages peuvent être constatés quant à l'utilisation de services de confiance :

- La sécurité et l'intégrité garanties des documents électroniques durant le processus d'interopérabilité (proposition et consommation des services);

- Le gain de temps, et l'économie d'argent;
- L'optimisation des processus d'interopérabilité;
- Les garanties juridiques.

2.5.6 Autorité de certification

L'autorité de certification (CA) délivre des certificats d'authentification et certificats de signature aux organisations membres. Tous les certificats sont stockés au sein du système de chaque membre. L'autorité de certification doit pouvoir traiter les demandes de signature de certificat conformes. Le CA doit distribuer les informations de validité du certificat via le protocole appelé OCSP⁷ (Online Certificate Status Protocol). Les serveurs de sécurité mettent en cache les réponses OCSP pour réduire la charge dans le service OCSP et augmenter la disponibilité. La charge sur le service OCSP dépend du nombre de certificats émis.

Une Autorité de Certification est une unité de confiance qui se situe au niveau de la base de la chaîne de certification électronique. Elle délivre et gère les certificats numériques qui seront utilisés pour la sécurité des échanges dématérialisés et pour garantir l'identité des institutions émettrices de messages.

Ainsi, l'Autorité de Certification émet des certificats électroniques qui sont sujets à :

L'identification :

L'identification est un processus ou une opération permettant d'établir l'identité de l'utilisateur. Elle permet de répondre à la question : "Qui êtes-vous ?". L'utilisateur utilise un identifiant (que l'on nomme "Compte d'accès", "Nom d'utilisateur" ou "Login" en anglais) qui l'identifie et qui lui est attribué individuellement. Cet identifiant est unique.

L'authentification :

Des certificats sont utilisés pour valider l'identité des émetteurs dans le cadre d'une procédure d'authentification, élément crucial de la sécurité des réseaux informatiques : ce sont les certificats d'authentification.

Le chiffrement :

Entre autres, on distingue les certificats SSL⁸ qui garantissent la sécurité et l'intégrité des informations échangées entre un site web et un navigateur, par le biais d'une clé cryptographique

⁷ OCSP signifie Online Certificate Status Protocol. En français, "protocole de vérification de certificat en ligne". Il s'agit d'un protocole de navigation qui permet de vérifier la validité d'un certificat SSL à l'aide d'une liste blanche.

⁸ Secure Sockets Layer (SSL) est un protocole de sécurité qui assure la confidentialité, l'authentification et l'intégrité des communications sur Internet. SSL a finalement évolué vers Transport Layer Security (TLS).

permettant d'activer une session sécurisée (protocole HTTPS⁹) : ce sont les certificats de chiffrement.

Une Autorité de Certification valide l'identité d'un demandeur et se porte garante de cette identité par le biais de l'émission d'un certificat électronique. Une fois la signature électronique apposée, il sera garanti que la clé publique appartient bien au demandeur qui l'a générée. Seule la clé publique certifiée peut fonctionner avec la clé privée appartenant au demandeur.

Enfin, l'Autorité de Certification gère le cycle de vie des certificats. Elle s'assure que ces derniers soient renouvelés ou révoqués (selon les conditions de renouvellement en vigueur), les certificats électroniques ayant une durée de validité limitée.

2.5.7 Autorité d'horodatage

L'autorité d'horodatage est l'unité qui s'assure que les données et services de bases traités ou sauvegardés sont bien rattachés à une date et une heure synchronisées avec un serveur de temps. Le but est de prouver que ces services de base et données ont bien existé avant une date précise.

Ainsi, s'il y aura procédure judiciaire, la date et l'heure rattachée à chaque service ou données feront l'objet de preuve de bonne foi des documents pour lesquels il est essentiel de certifier que certaines données et/ou services ont bel et bien existés à un moment donné, dans la forme où ils ont été présentés à l'autorité d'horodatage.

2.6 Catalogue des services d'interopérabilité

Un catalogue des services d'interopérabilité a pour objet de structurer et présenter les services communs et récurrents qui peuvent être consommés et utilisés par chaque membre de l'écosystème d'interopérabilité, entre-autres l'authentification, la signature électronique etc.

La liste des services proposés et disponibles dans le catalogue n'est pas exhaustive; en effet, il évolue en fonction des besoins et des enjeux des membres de l'écosystème par rapport à la nécessité de mutualiser des services.

2.7 Architecture

L'administration publique exige la prestation de services efficaces qui ajoutent de la valeur aux citoyens. Les services publics doivent être améliorés et connectés en tenant compte du fait qu'ils ont été initialement conçus pour fonctionner de manière isolée. Chaque entité conçoit son modèle de gestion des services en tenant compte des réglementations en vigueur dans son secteur. Il y a peu de

⁹ HTTPS veut dire HyperText Transfer Protocol Secure (protocole de transfert hypertextuel sécurisé), et c'est la version chiffrée du HTTP. Il est utilisé pour sécuriser les communications sur internet ou sur un réseau. Le protocole de communication est chiffré au moyen de la TLS (Transport Layer Security) ou, auparavant, de la SSL (Secure Sockets Layer)

coordination entre les entités du même secteur ou domaine de service au citoyen et cette coordination est encore moins entre les différents secteurs.

Pour initier un processus de changement qui permette un travail coordonné entre les entités pour concevoir de meilleurs services, il est nécessaire d'avoir une architecture des systèmes interopérables comme représentée par la Figure 2.

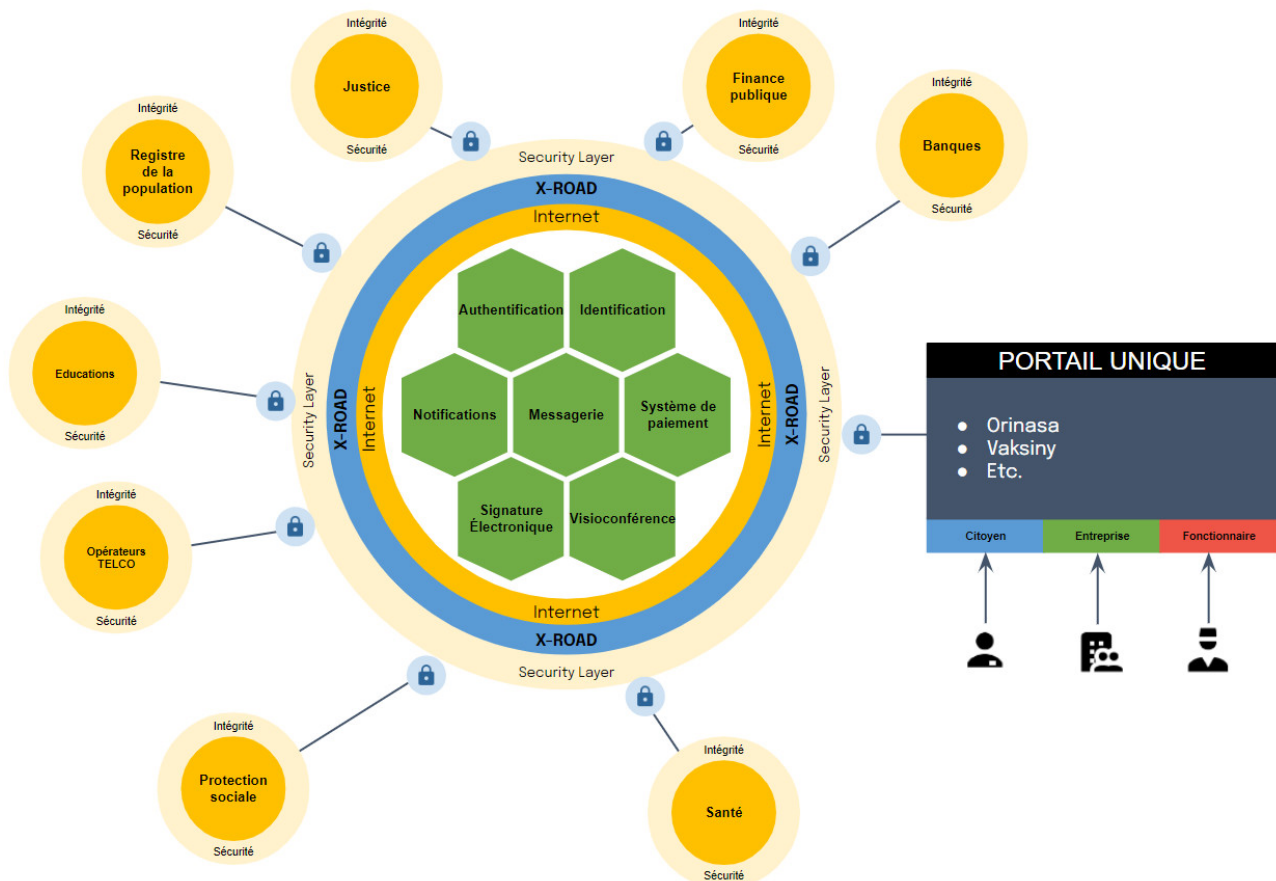


Figure 2: Architecture des services publiques

En général, ce modèle d'architecture des services publics représenté par la Figure 2 est un ensemble d'outils qui permettent aux entités publiques de :

- Identifier les composantes d'un service gouvernemental;
- Montrer comment les composants d'un service s'empilent;
- Appliquer des normes, des outils et des pratiques exemplaires;
- Mettre en œuvre les parties indépendantes d'un gouvernement connecté.

L'architecture comprend des actions pour les différents domaines de gestion des entités, ceci pour aligner les efforts entre les différentes entités. L'architecture adoptée pour les administrations publiques, qui continue d'évoluer, répond très bien aux besoins des entités.

2.8 Technologie

Les solutions informatiques doivent répondre aux besoins de flux de travail et de gestion des données des services publics. Pour concevoir des solutions informatiques supportant des services intégrés, il est nécessaire d'utiliser des normes et des technologies sans restriction d'utilisation et d'accès libre, supportées par des communautés de pratique. L'utilisation de normes garantit le couplage entre différentes solutions et elles sont indépendantes de la technologie utilisée.

Pour tout cela, le principal canal de livraison de la fonctionnalité d'une application gouvernementale est une API, en tenant compte des différentes manières dont elle peut être invoquée et des cas d'utilisation possibles.

De plus, pour garantir l'expérience utilisateur, les solutions de gouvernance doivent pouvoir fonctionner en mode hors ligne (offline first) jusqu'à ce qu'une connexion soit rétablie.

En effet, la plateforme d'interopérabilité doit fournir la confiance et la sécurité, en respectant les principes et exigences :

- Elle doit fournir la confiance et la sécurité par la présence d'une autorité de certification, de signature et d'horodatage pour garantir le cadre de confiance sur l'ouverture, la réutilisabilité, la sécurité et la confidentialité des données à tous les acteurs ;
- Elle permet de tracer les données ou informations qui transitent dans l'écosystème. Ce qui garantit la transparence et la traçabilité de son utilisation ;
- Elle supporte des interfaces (Application Programming Interface ou API) qui constituent des services répondants aux besoins des utilisateurs finaux ;
- Elle favorise le développement des services publics et privés accessibles à tous les citoyens ;
- Elle est une couche d'échange permettant la communication entre les systèmes, indépendamment de leur choix technologique tout en étant flexible et agile facilitant ainsi l'évolution de l'écosystème interopérable ;
- Elle réduit les charges administratives en permettant la mise en œuvre de "once only principle" ;
- Elle constitue une passerelle permettant le partage de données ou informations pour garantir la conservation de la lisibilité, la fiabilité et l'intégrité des informations. Son système permet l'accessibilité aussi longtemps que nécessaire, sous réserve des dispositions en matière de sécurité et de confidentialité ;
- Elle permet la prévention des risques et des impacts grâce à sa stabilité.

Ainsi la solution technologique choisie qui répond à ces principes est **X-ROAD**¹⁰. Il s'agit d'une plateforme de l'e-gouvernance open source et une solution d'écosystème qui fournit un échange de données unifié et sécurisé entre les organisations.

III. DIRECTIVES ET RÈGLES OPÉRATIONNELLES

3.1 Evaluation de la préparation à l'interopérabilité

Pour préparer la pratique de l'interopérabilité, il est nécessaire d'analyser la situation actuelle et d'en faire le diagnostic afin de pouvoir identifier les obstacles éventuels ainsi que les possibilités de solutions à adopter.

Dans ce sens, différentes métriques et approches d'évaluation ont été définies. Ces approches peuvent être considérées comme suit :

- niveau de maturité de l'interopérabilité et de l'environnement hébergeant les systèmes d'information étudiés ;
- degré de compatibilité des interfaces externes des systèmes d'information entre eux ;
- la performance opérationnelle de l'interopérabilité en tenant compte des trois critères suivants : qualité, coût et délai.

Ainsi, les conditions suivantes doivent être vérifiées pour chaque entité qui veut devenir membre du système d'interopérabilité de Madagascar.

- L'entité est-elle consciente du changement apporté par l'interopérabilité ?
- Existe-t-il une entité pour accompagner les nouveaux membres ?
- A quel niveau se situe la connaissance et la compétence de l'entité vis-à-vis du système d'interopérabilité ?
- A quel niveau se situe l'aptitude de l'entité à assimiler et utiliser les documentations en vigueur (guides, manuels, cadre, normes et standards...) ?
- A quel niveau se situe la capacité de l'entité à mener à bien les activités nécessaires pour réussir l'interopérabilité ?

Pour mieux évaluer la préparation d'une entité pour l'interopérabilité, une matrice dite "Matrice de Traçabilité des Exigences" doit être remplie par celle-ci.

¹⁰ X-Road est une couche d'échange de données entre des systèmes d'information. Les organisations peuvent échanger des informations par Internet à l'aide de X-Road pour garantir la confidentialité, l'intégrité et l'interopérabilité entre les parties prenantes de l'échange de données. X-Road est administrée de manière centralisée mais distribuée.

3.2 Approche Orientée Service

L'enjeu est d'avoir un écosystème interopérable et agile. En effet, il faut que chaque entité puisse proposer un catalogue de services permettant de faire dialoguer chaque système applicatif de l'écosystème. Pour un écosystème Agile, il est nécessaire de diminuer l'interdépendance entre chaque entité, facilitant ainsi la réutilisation, le partage et l'évolution des services.

L'architecture de chaque système applicatif doit respecter une architecture orientée service. Elle doit, par ailleurs, respecter les normes et standards d'interopérabilité en vigueur.

3.3 Conformité de l'interopérabilité entre entités

Afin de déterminer qu'une opération de mise en place d'interopérabilité entre entités suit bien les normes et standards imposés, il faut qu'elle soit conforme à des critères d'interopérabilité. Cette conformité doit être validée par l'UGD.

Une matrice d'exigences doit être définie afin d'établir une notation servant de critères pour la validation.

3.4 Outils pour la mise en œuvre de l'interopérabilité

3.4.1 Cartographie du Système d'information

La Cartographie du Système d'Information est constituée des éléments suivants :

- une représentation **des processus métier** organisant les activités;
- un **modèle d'activités** permettant d'identifier les fonctions gérées par les applications;
- un **modèle d'objets métier** identifiant les données métier.

Pour avoir ces éléments qui sont indispensable à la mise en œuvre de l'interopérabilité, il est recommandé :

- d'avoir une visibilité sur le partage des fonctionnalités entre l'ensemble des acteurs concernés;
- d'élaborer des standards d'échange alignés sur un modèle d'objets métier faisant consensus;
- de faire une analyse d'impact pour passer d'un existant vers un modèle cible d'interopérabilité.

3.4.2 Modèle d'interopérabilité

Le modèle d'interopérabilité du Système d'information est un modèle de référence d'échange d'informations commun, assurant que toutes les applications puissent interagir sans conflits sémantiques (signification, interprétation).

Le modèle d'interopérabilité identifie les services numériques, les données échangées et les briques techniques requises (traçabilité, sécurité) pour le Système d'information. Il est implémenté sous la forme d'un socle d'interopérabilité mis à disposition de tout système souhaitant échanger dans le respect des principes d'interopérabilité.

Il précise les cas d'usage relatifs aux échanges entre systèmes participants, sur les échanges candidats à une interopérabilité partagée.

Il couvre l'interopérabilité horizontale (entre outils de processus différents) et l'interopérabilité verticale (entre outils d'un même processus).

IV. DIRECTIVES À SUIVRE

Le présent chapitre revêt une importance centrale et capitale dans le cadre d'interopérabilité dans la mesure où il contient une série de directives concrètes qui visent à optimiser l'interopérabilité et qui s'appliquent à tous les organismes du secteur public. Ces directives sont présentées en les structurant en fonction des principes, des niveaux d'interopérabilité et des éléments sur la gouvernance de l'interopérabilité.

4.1 Transparence

Directive n°1	Créer la transparence nécessaire quant aux règles administratives et aux processus qui s'y appliquent, aux données, aux démarches ou aux services qui sont disponibles.
Directive n°2	Mettre à disposition dans la mesure du possible des interfaces ouvertes qui permettent à d'autres d'accéder aux services.

4.2 Réutilisabilité

Directive n°3	Réutiliser et partager les services, et collaborer au développement de services conjoints.
Directive n°4	Réutiliser et partager les informations et données lors de la mise en œuvre de services, sauf lorsque des restrictions en matière de confidentialité ou de respect de la vie privée s'appliquent.
Directive n°5	Mettre en place une base commune de services et de sources d'informations (sources authentiques, données ouvertes, etc.) réutilisables qui peuvent être utilisées par différents utilisateurs concernés.
Directive n°6	Rendre accessibles à des tiers les sources d'information faisant autorité (sources authentiques), tout en mettant en œuvre des mécanismes d'accès et de contrôle permettant d'en assurer la sécurité et la confidentialité, conformément à la législation applicable.

Directive n°7	Communiquer clairement le droit d'accès et de réutilisation des données
Directive n°8	Développer des interfaces avec les registres de base et les sources d'information faisant autorité (sources authentiques)

4.3 Centré sur l'utilisateur

Directive n°9	Utiliser, si cela est dans l'intérêt de l'utilisateur, plusieurs canaux pour fournir les services, démarches ou contenus afin que les utilisateurs puissent choisir celui qui convient le mieux à leurs besoins.
---------------	--

4.5 Sécurité, confidentialité et intégrité

Directive n°10	Définir un cadre commun de sécurité et établir des processus applicables aux services afin d'assurer des échanges de données sûrs et fiables entre les organismes du secteur public et lors de leurs interactions avec les citoyens et les entreprises.
Directive n°11	Utiliser des solutions techniques favorisant la portabilité vers les utilisateurs.

4.6 Neutralité technologique et portabilité des données

Directive n°12	Garantir, lorsque cela est légalement possible et en n'imposant pas de restrictions injustifiées, la portabilité des données, c'est-à-dire le transfert facile des données entre services.
----------------	--

4.7 Simplification administrative

Directive n°13	Simplifier les processus et utiliser, chaque fois que c'est approprié, des modes d'accès numériques pour la fourniture de services, afin de fournir une réponse rapide et de qualité aux demandes des utilisateurs et de réduire la charge administrative pesant sur les organismes du secteur public, les entreprises et les citoyens.
----------------	---

4.9 Évaluation de l'efficacité et de l'efficience

Directive n°14	Évaluer l'efficacité et l'efficience des différentes solutions d'interopérabilité et options technologiques en tenant compte des besoins des utilisateurs et du rapport entre coûts et qualités.
----------------	--

Références

- 1) Direction Interministérielle du Numérique et du Système d'Information et de Communication de l'Etat (FRANCE). Référentiel Général d'Interopérabilité. Disponible dans https://www.numerique.gouv.fr/uploads/Referentiel_General_Interopabilite_V2.pdf;
- 2) Gouvernement du Maroc. Cadre Général d'Interopérabilité. Disponible dans http://www.egov.ma/sites/default/files/cgi_2012_v1.pdf
- 3) Agence des services et systèmes d'information- présidence de la République du Bénin, Plateforme nationale d'interopérabilité. Disponible dans <https://www.xroad.bj/publications/documents>;
- 4) Gouvernement du Québec. Cadre commun d'interopérabilité. Disponible dans https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/cadre_commun_interoperabilite.pdf
- 5) Ministère du Développement de l'Economie Numérique et des Postes du Burkina -Faso. Référentiel Général d'Interopérabilité. Disponible dans https://www.dgtic.gov.bf/wp-content/uploads/2020/03/Document-RGI-version-1.0-version-a_dopt%C3%A9-Mai-2018.pdf
- 6) Congrès international de génie industriel. Disponible dans https://www.researchgate.net/publication/278804374_Developpement_de_l'interopabilite_des_applications_de_gestion_industrielles_concepts_de_base_et_definitions
- 7) X-ROAD® Organizational Model
https://x--road-global.translate.google/X-ROAD-organizational-model?_x_tr_sl=en&_x_tr_tl=fr&_x_tr_hl=fr&_x_tr_pto=sc
- 8) Ministère de l'Economie, des Finances et de la Souveraineté Industrielle et Numérique de la France, Cadre Commun d'Interopérabilité de la Commande Publique disponible sur https://www.economie.gouv.fr/files/files/directions_services/commande-publique-numerique/Ressources/Documentation/Cadre_commun_dinteroperabilite.pdf
- 9) Ministère de la Digitalisation Luxembourg disponible sur <https://digital.gouvernement.lu/fr/publications/document-de-reference/NIF-2019/NIF-2019.html>