CADRE D'INTEROPÉRABILITÉ

Unité de Gouvernance Digitale - UGD

https://digital.gov.mg

Etat	Version	Date de la version
En cours de validation	0.2	22 Décembre 2021

VERSIONS DU DOCUMENT

Version	Date	Auteur/Fonction : Nom	Objet de la mise à jour
0.1	Déc 2021	AMOA/PO/Architecte SI	Création
0.2	Mars 2022	AMOA/PO/Architectes SI	Amélioration continue
0.3	Mars 2022	AMOA/PO/Architectes SI	Intégration retour WB

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**

DOCUMENTS DE RÉFÉRENCE

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

LISTE DES ABREVIATIONS

API : Application Programming Interface

CA : Certificate Authority (autorité de certification)

CIRT : Computer Incident Response Team

CMIL : Commission Malagasy de l'Informatique et des Libertés

DMZ : Zone Démilitarisée

HTTPS : HyperText Transfer Protocol Secure

ID : Identification

JSON : JavaScript Object Notation

LAN : Local Area Network

OCSP : Online Certificate Status Protocol

REST : Representational State Transfer

RGPD : Règlement Général sur la Protection des Données

SMS : Short Message Service

SOAP : Simple Object Access Protocol

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

1.1 Contexte et objectifs

1.1.1. Contexte générale

Actuellement, plusieurs enjeux, notamment sociaux, humains et économiques sont touchés par la transformation digitale dans le monde. Elle est devenue, sans doute, un levier de développement pour tous les types d'organisations, que ce soit publique ou privée. De plus en plus de pays adoptent actuellement la digitalisation de leurs services publics dans le but de gagner du temps, de l'argent et plus d'efficacité.

De ce fait, le gouvernement malagasy, par le biais de l'**e-gouvernance**, 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 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

Suivant l'objectif principal qui est d'avoir, en 2024, au moins cinq million (5.000.000) d'utilisateurs bénéficiant de services conformes aux normes de services, un des objectifs spécifiques imposés par la politique de digitalisation s'avère d'**augmenter le nombre de systèmes conformes aux normes nationales d'interopérabilité**. Dans ce cas, il faut que plusieurs institutions soient interopérables entre elles. Des normes et standards doivent être connues et suivies pour une interopérabilité parfaite entre les institutions. Alors, l'établissement d'un cadre d'interopérabilité se trouve être une étape indispensable. Le but du développement de ce cadre d'interopérabilité est, en premier lieu, de mettre en œuvre un processus qui permet de déterminer des besoins et/ou des problèmes d'interopérabilité entre deux ou plusieurs entités, afin de trouver une ensemble de solutions qui pourraient résoudre ces problèmes ou besoins. En outre, ce cadre servira de guide pour toutes les parties prenantes lors de l'application des normes et standards d'interopérabilité (contenus dans un document déjà élaboré).

Par ailleurs, l'objectif est aussi de faciliter la mise en œuvre de l'interopérabilité dans le cadre de l'e-gouvernance, par le biais de :

- l'assurance de la sécurité et la confidentialité, ainsi que la détermination de la propriété des données;
- renforcement de la capacité institutionnelle (matériaux, humains) de prestation de services multicanaux;
- principe "once-only" à tous les services;
- la mise en place de l'écosystème de données et de réglementation qui permet l'application du développement du cadre institutionnel et les plateformes technologiques qui permettent l'échange de données (X-ROAD), l'accès numérique, les paiements, les signatures et les notifications;

- mise en place de l'infrastructure nécessaire au travail à distance et à la connectivité entre les unités de l'administration centrale à l'intérieur de la capitale ainsi que dans les régions les plus reculées.

1.1.3. Résultat attendu

Le résultat à court terme est d'avoir, dans un premier temps, un **Cadre d'Interopérabilité** permettant de renforcer la vision d'unité de l'État, en ayant une plus grande capacité de communiquer, de fournir et d'utiliser des services d'administration numériques efficaces pour améliorer la qualité de vie des citoyens. Le Cadre d'Interopérabilité est le document qui accompagne les entités dans le développement de leurs capacités d'échange d'informations, indépendamment de ses restrictions ou sa taille. Il constitue donc un document de référence et de normalisation pour les administrations (publiques et privées) Malagasy. Il liste les règles de conformité à propos de l'usage des normes, des standards ou encore des références dans le développement des systèmes d'informations. Pour cela, un consensus à propos de l'application de ces normes et règles devra être trouvé entre les parties prenantes, sachant que l'Unité de Gouvernance Digitale œuvrera en appui.

Par ailleurs, un des résultats attendus est aussi d'assurer une sécurité ainsi que de mettre en place une grande confiance entre les institutions de l'écosystème interopérable. Les éléments qui les permettent seront vus dans ce document cadre.

1.2 Définitions

Avant de voir les différents points essentiels à un cadre d'interopérabilité, il est idéal de voir 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, de se comprendre l'un et l'autre ainsi que de fonctionner en synergie. C'est donc un ensemble de règles, basées sur des normes et standards, permettant aux institutions publiques et privées de partager l'information entre eux et avec les usagers afin d'intégrer cette information au sein de processus métiers dématérialisés.

L'interopérabilité est rendue possible par :

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

C'est la structure de travail commune où les concepts et les critères guident l'échange d'informations.

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 entre structures de l'administration publique et privée en vue de la mise en place de services via un portail unique.
Le cadre d'interopérabilité sert de guide et référentiel pratique à toute entité (publique ou privée), qui doit ou souhaite mettre en œuvre un système interopérable pour offrir un service.

1.3 Champs d'application du cadre d'interopérabilité

En vue d'une gouvernance digitale optimale, il faudrait toucher le maximum de domaines. Ainsi, nous allons commencer par les finances publiques, en passant par la santé et l'éducation, jusqu'au secteur commercial public et surtout privé. De ce fait, plusieurs champs d'application peuvent être sujets du cadre d'interopérabilité, à savoir : Création d'entreprise en ligne, Paiement d'impôts en ligne, Candidature en ligne, Santé, Éducation, Assurances…

1.4 Public cible du cadre d'interopérabilité

Le public cible de ce document (cadre d'interopérabilité) sont les institutions publiques et privées qui souhaitent :

- consommer un ou plusieurs services proposés (fournis) par d'autres institutions;
- proposer (fournir) un ou plusieurs services qui pourront être consommés par d'autres institutions.

Ces institutions sont principalement les parties prenantes de la gouvernance digitale. Elles sont donc les responsables de la mise en œuvre de la stratégie numérique dans l'administration publique, les registres d'entreprises et l'interopérabilité. Toutefois, la participation des entreprises du secteur privé est vivement sollicitée.

II. CADRE D'INTEROPÉRABILITÉ

2.1 Les principes fondamentaux d'interopérabilité

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

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.

Cela comprend les interfaces avec les systèmes d'information internes qui facilitent la réutilisation des systèmes et des données et garantissent le droit à la protection des données à caractère personnel en respectant les cadres politiques, juridiques et organisationnels applicables aux volumes importants de données à caractère personnel et gérés par les administrations publiques.

Principe 2 : Réutilisabilité

Les administrations publiques nécessitant un besoin spécifique, cherchent une solution parmi celles déjà disponibles, à portée de main, qui ont fait leurs preuves 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 sont priorisés lors de la détermination des services publics à fournir et de la manière dont ils 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 multicanal (disponibilité de canaux alternatifs, physiques et numériques, pour accéder à un service), est un élément important de la conception du service public, car les utilisateurs peuvent préférer différents canaux en fonction de leur situation et de leurs besoins.

• Un point de contact unique doit être mis à la disposition des usagers, pour masquer la complexité administrative interne et faciliter l'accès aux services publics.

• Les commentaires des utilisateurs doivent être systématiquement recueillis, évalués et utilisés pour concevoir de nouveaux services publics et améliorer ceux qui existent déjà.

Principe 4 : Inclusion et accessibilité

La livraison inclusive permet à chacun de tirer pleinement parti des opportunités offertes par les nouvelles technologies pour accéder et utiliser les services numériques, en surmontant les fractures et l'exclusion sociales et économiques.

L'accessibilité garantit que les personnes handicapées, les personnes âgées et les autres groupes défavorisés peuvent utiliser les services publics à des niveaux de service comparables à ceux fournis aux autres citoyens.

L'inclusion et l'accessibilité impliquent généralement une diffusion multicanale. La prestation de services traditionnelle sur papier ou en personne devra peut-être coexister avec la prestation électronique. L'inclusion et l'accessibilité peuvent également être améliorées par la capacité d'un système d'information à permettre à des tiers d'agir au nom de citoyens qui ne sont pas en mesure, de manière permanente ou temporaire, d'utiliser directement les services publics.

Principe 5 : 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 et digne de confiance et dans le plein respect des normes et réglementations applicables. Les administrations publiques doivent garantir la disponibilité, la confidentialité, l'authenticité, l'intégrité et la non-répudiation des informations fournies par les citoyens et les entreprises. Chaque administration est aussi responsable de tous les actes 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, de manière périodique, de toutes ces données d’accès. Il est important de responsabiliser le(s) point(s) focal(aux) de chaque institution sur l’importance des accès que l’on va lui/leur confier. L’objectif est de toujours assurer la sécurité et la confidentialité de tout l’écosystème interopérable Malagasy. Ceci nécessite un sens de l’anticipation et une vigilance de la part de chaque institution qui fait partie de l’écosystème.

Principe 6 : 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 également pouvoir être réutilisées dans différents systèmes.

Principe 7 : 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, y compris 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.

•Digital-first, 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 multicanal, comme la coexistence de canaux physiques et numériques.

Principe 8 : Préservation des informations

Les données doivent être stockées et accessibles pendant un temps déterminé. Cela signifie que les enregistrements et les informations sous forme électronique détenus par les administrations publiques doivent être conservés et convertis, si nécessaire, sur de nouveaux supports lorsque les anciens supports deviennent obsolètes. L'objectif est de s'assurer que les dossiers et autres formes d'information conservent leur lisibilité, leur fiabilité et leur intégrité et qu'ils sont accessibles aussi longtemps que nécessaire, sous réserve des dispositions en matière de sécurité et de confidentialité.

Principe 9 : Évaluation de l'efficacité et de l'efficience

Pour évaluer l'efficacité et l'efficience de l'interopérabilité, il faut 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, l'amélioration du fonctionnement méthodes et niveau de satisfaction et impacts sur les utilisateurs.

2.2. Catalogue de services

Le catalogue de services est une liste des services de base (Application Programming Interface ou API) où une entité (en tant que fournisseur de services) va mettre son/ses service(s) à disposition d'une autre qui veut le(s) consommer. Ce catalogue constitue un sous-ensemble du portefeuille de services et ne doit comprendre que les services actifs et disponibles, qui suivent les normes et standards d'interopérabilité en vigueur.

En tant qu'outil d'interopérabilité entre les institutions, le catalogue de services doit se présenter sous la forme d'un document (national) mis en forme, facile à manipuler et à lire par toutes les institutions membres de l'interopérabilité auxquelles il est destiné.

Le catalogue de service décrit, donc, les services de base qui sont déjà disponibles et réutilisables. Ceci a pour but d'améliorer leur utilisation et leur accessibilité. Ce composant permet aux institutions propriétaires de services de documenter et de mettre à disposition des ressources qui pourront être réutilisées par d'autres institutions.

Il s'agit, d'une part, d'un outil pour coordonner les systèmes d'informations des institutions publiques. D'autre part, c'est un outil de développement, d'administration de systèmes et de support pour la maintenance des services de base et des données de référence.
Ainsi, chaque service du catalogue doit être décrit et présenté avec les informations suivantes :

- Un code ou identifiant unique du service;
- Le nom ou libellé du service;
- Une description détaillée du service ;
- Le champs d'application auquel le service appartient;
- La plage d'ouverture du service;
- Les conditions d'utilisation du service.

Son but est de garantir la gestion efficace, transparente et équilibrée des systèmes d'information des institutions publiques.

Le catalogue de services de base aide à planifier la gestion de l'information de l'administration publique. Par ailleurs, il fournit des informations sur les sujets suivants :

- Les Systèmes d'information, service de base et base de données qui sont mis en œuvre dans les institutions public;
- Les données collectées et traitées dans les systèmes d'information;
- Les services de base fournis et leurs utilisateurs;
- Les responsables, les processeurs autorisés des systèmes d'information, les services de base, les bases de données et les personnes de contact;
- La base juridique que permet d'exploiter et de traiter les services de base et les bases de données;
- Les composants réutilisables garant de l'interopérabilité des systèmes d'information (XML, JSON etc., dictionnaires);

Le catalogue de services de base permet à l'environnement administratif de :

- Enregistrer et approuver les systèmes d'information, les services de base et les bases de données ;
- Enregistrer les connexions à la plateforme d'interopérabilité;
- Administrer les composants réutilisables (webservices, API, XML, JSON…).

Ainsi, les institutions propriétaires des données publient les services de base correspondants dans le catalogue. Elles autorisent, par le biais de la plateforme, les autres institutions consommatrices à les utiliser dans leurs systèmes d'informations.

2.3 Gouvernance des données et Once Only Principle

2.3.1. Gouvernance de données

Les données sont un élément fondamental 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 dans le cadre de l'interopérabilité ;
- **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 en vigueur, notamment le Règlement général sur la protection des données (RGPD) ;
- **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 institutions 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 institutions publiques ou privées qui vont faire partie de l'interopérabilité ne devraient avoir à fournir leurs services qu'une seule fois dans leurs échanges, c'est le "Once Only Principle".

2.3.2. 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 institutions 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 Madagascar est d'appliquer le principe unique (once only). 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 transmises qu'une seule fois aux administrations publiques, mais que 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.

2.4 Modèle organisationnel

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

- Une autorité de gouvernance (UGD);
- Un comité national d'interopérabilité
- Institutions membres (à la fois les fournisseurs et consommateurs de services);
- Responsable CIRT et CMIL;
- Une Comité d'architecture (national et sectoriel);
- Service de confiance.
- Une autorité de certification
- Une autorité d'horodatage

2.4.1 Autorité de gouvernance

Étant le centre de l'écosystème d'interopérabilité de Madagascar, l'autorité de gouvernance sera assurée par l'UGD, au début et sera responsable de tous les aspects des opérations. Les responsabilités comprennent la définition des réglementations et des pratiques, l'acceptation de nouveaux membres, l'assistance aux membres et l'exploitation des composants centraux du logiciel 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.

2.4.2 Comité National d'Interopérabilité

A long terme, il devrait y avoir un **Comité national d'Interopérabilité** qui doit impliquer toutes les parties prenantes de l'interopérabilité à Madagascar. Ce comité 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. Ainsi, le management de l'écosystème d'interopérabilité malagasy sera donc assuré par le Comité d'interopérabilité. Ceci dans le but de faire respecter la normalisation ainsi que d'assurer une pérennité de l'écosystème.

2.4.3 Institutions 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. 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 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.

2.4.4 CIRT & CMIL

2.4.4.1. CIRT (Computer Incident Response Team) :

La CIRT-MDG assurera la gouvernance de l'aspect important des fonctions régaliennes de l'État en termes de protection des données nationales. La CIRT Nationale a un rôle crucial à jouer dans ce contexte en ce qu'elle organise et coordonne toutes les actions allant du répertoriage des acteurs à tous les niveaux, la dispense de conseil pour la riposte en cas d'attaque cybernétique individuelle ou collective à la détermination des actions de nature économique idoines nées des retombées positives suite à une prise en main efficace de la question de cybermenace.

2.4.4.2. CMIL (COMMISSION MALAGASY DE L'INFORMATIQUE ET DES LIBERTÉS) :

La CMIL a pour missions de :

- informer toutes les personnes concernées sur leurs droits et obligations, et protéger ces droits ;
- veiller à la mise en conformité des traitements des données à caractère personnel ;
- délivrer des autorisations et des labels ;
- contrôler et prononcer des sanctions administratives en cas de non-respect des principes posés pour le traitement des données.

Pour réaliser ses missions, la CMIL a le pouvoir de :

- émettre des recommandations ;
- prendre des décisions individuelles ou réglementaires ;
- adopter des mesures de correction ;

- prononcer des sanctions pécuniaires.

2.4.5 Comités d'architecture

Les travaux d'interopérabilité nécessitent l'intervention de deux types de comités

- **Le Comité national** qui définit la stratégie nationale en termes d'Architecture d'Entreprise Gouvernementale. Il s'agit du Comité qui coordonne d'une part l'ensemble des architectures de toutes les institutions membres de l'interopérabilité malagasy, et d'autre part l'Architecture d'Entreprise Gouvernementale proprement dite.
- **Le Comité sectoriel** qui se charge de la stratégie du Système d'information au niveau d'une entité précise en coordination avec la direction des systèmes d'information de l'institution et le comité national.

2.4.6 Services de confiances

Les Services de Confiance permettent :

- La création, la vérification et la validation :
    - 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

Ce prestataire met en place, auprès des parties prenantes de l'interopérabilité, des mécanismes d'identification électronique sécurisés (régi 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 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 garantie 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.

2.4.7 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 OCSP (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'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 SSL qui garantissent la sécurité et l'intégrité des informations échangées entre un site web et un navigateur, par le biais d'une clé cryptographique permettant d'activer une session sécurisée (protocole HTTPS) : 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.

2.4.8 Autorité d'horodatage

L'autorité d'horodatage est l'unité qui s'assure que les données et services de bases traités ou sauvegardées 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.

2.5 Services partagés

Il s'agit de services communs qui peuvent être consommés par chaque membre de l'écosystème d'interopérabilité. Pour notre cas, il y a les services : authentification, signature électronique et e-paiement.

2.5.1. ID authentification (authentification unique)

L'authentification unique, souvent désignée par le sigle anglais SSO (de single sign-on) est une méthode permettant à un utilisateur d'accéder à plusieurs applications informatiques (ou sites web sécurisés) en ne procédant qu'à une seule authentification.

Les objectifs sont :

- simplifier pour l'utilisateur la gestion de ses mots de passe ;
- simplifier la gestion des données personnelles détenues par les différents services en ligne, en les coordonnant par des mécanismes de type méta-annuaire ;
- simplifier la définition et la mise en œuvre de politiques de sécurité.

Les avantages de l'authentification unique incluent :

1. la réduction de la fatigue de mot de passe : manque de souplesse liée à l'utilisation de différentes combinaisons de nom d'utilisateur et de mot de passe ;
2. la réduction du temps passé à saisir le même mot de passe pour le même compte ;
3. la réduction du temps passé en support informatique pour des oublis de mots de passe;
4. la centralisation des systèmes d'authentification ;
5. la sécurisation à tous les niveaux d'entrée/de sortie/d'accès aux systèmes sans sollicitation multiple des utilisateurs ;
6. la centralisation des informations de contrôles d'accès pour les tests de conformités aux différentes normes.

2.5.2. Signature électronique

C'est la **transposition numérique** d'une signature manuscrite sur un document. Elle engage le consentement du signataire de la même manière que la signature manuscrite. Elle permet à l'administration publique de **dématérialiser la signature contractuelle**. Tous types de documents peuvent être signés numériquement.

La signature électronique est sécurisée par le biais d'une fonction de cryptographie, dite de « hashing ». Elle permet de v**érifier l'identité** du signataire et **l'intégrité** du document. Des systèmes de sécurité

complexes garantissent l'identité de ce dernier. En effet, l'authentification doit faire l'objet de contrôle à plusieurs facteurs pour assurer une niveau de sécurité élevé et fiable (par exemple : authentification par carte, ou par device…).

La signature électronique assure également la **traçabilité** des documents signés, et empêche toute modification à postériori via un certificat électronique. Elle permet ainsi **d'approuver** des documents, de **garantir** l'identité du signataire, et **l'intégrité** des documents.

Trois (03) niveaux de fiabilité de la signature électronique sont prévus :

- 1. **Simple** qui est représenté sous la forme d'une case à cocher. Il permet à l'utilisateur de valider la conformité du document;
- 2. **Avancée** qui répond à des critères spécifiques. La signature électronique doit être **rattachée exclusivement au signataire** et permettre son identification. Le signataire garde sous son contrôle exclusif la procédure de création de sa signature électronique. Celle-ci doit être **liée aux données auxquelles elle se rattache**, de sorte que toute modification sur les dites données soit détectable;
- 3. **Qualifiée** qui repose sur un **certificat qualifié de signature électronique**. Il s'agit du niveau de fiabilité le plus élevé. Seule la signature électronique qualifiée dispose d'une **présomption de fiabilité**. En cas de litige, celui qui conteste la signature électronique qualifiée doit apporter la preuve de la défaillance des dispositifs techniques.

2.5.3. e-Paiement

Le e-paiement désigne l'intégralité des transactions étant réalisées à partir d'un ordinateur, tablette, smartphone, etc. Il concerne tous les paiements effectués par le biais d'internet ou par réseau téléphonique.

L'e-paiement nous permet :

- **Le gain de temps :** Le e-paiement permet un gain de temps considérable tant du côté du payeur que du côté du receveur. C'est une possibilité appréciée dans les deux camps.
- **La simplicité :** En quelques clics, les payeurs peuvent effectuer la transaction. Cela nous permet d'éviter l'utilisation des chéquiers qui risquent parfois aux chèques sans provision et des virements à effectuer depuis son compte qui nécessitent un déplacement auprès de l'agence la plus proche. Du côté du receveur, moins de manipulations sont à effectuer également : les données sont mises à jour de manière automatique et permettent donc une réduction de l'intervention humaine et de facto du risque d'erreurs.
- **L'augmentation de paiement :** effectuer des paiements , même en dehors des horaires d'ouvertures du point de paiement.

2.6 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 institution conçoit son modèle de gestion des services en tenant compte des réglementations en vigueur dans son secteur. Il y a peu de

coordination entre les institutions 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 institutions pour concevoir de meilleurs services, il est nécessaire d'avoir une architecture des services publics comme représentée par la Figure 1.

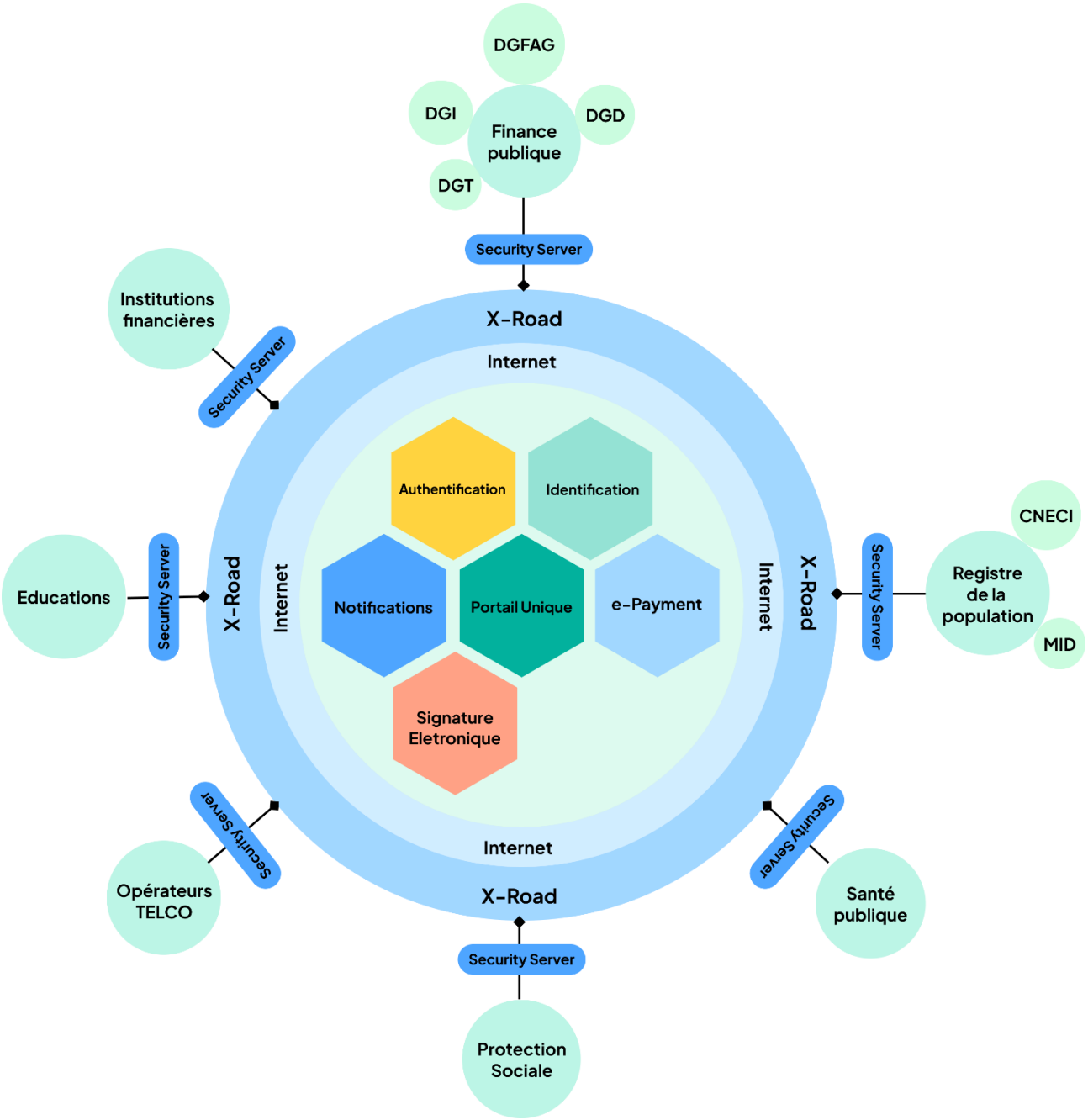

Figure 1: Architecture des services publiques

En général, ce modèle d'architecture des services publics représenté par la Figure 1 est un ensemble d'outils qui permettent aux institutions publiques de :

- Identifier les composantes d'un service gouvernemental;

- Montrer comment les composants d'un service s'emboîtent;
- 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 institutions, ceci pour aligner les efforts entre les différentes institutions. L'architecture adoptée pour les institutions publiques, qui continue d'évoluer, répond très bien aux besoins des institutions.

2.7 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 Programing 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 du principe de once only ;
- 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**. 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 institution qui veut devenir membre du système d'interopérabilité de Madagascar.

- L'institution 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'institution vis-à-vis du système d'interopérabilité ?
- A quel niveau se situe l'aptitude de l'institution à assimiler et utiliser les documentations en vigueur (guides, manuels, cadre, normes et standards...) ?
- A quel niveau se situe la capacité de l'institution 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.

3.2 Approche Orientée Service

L'enjeu est d'avoir un écosystème interopérable et agile. En effet, il faut que chaque institution 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 institution, 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 Evolution du Cadre d'interopérabilité

Au regard de l'évolution constante des technologies et des usages, le Cadre d'Interopérabilité devra être mis à jour si besoin. A cet effet, il est recommandé une révision annuelle**.**

3.4 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 le Comité National d'Architecture.

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

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_Interoperabilite_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-adopt%C3%A9e-Mai-2018.pdf

6) Congrès international de génie industriel. Disponible dans https://www.researchgate.net/publication/278804374_Developpement_de_l'interoperabilite_des_applications_de_gestion_industrielles_concepts_de_base_et_definitions

7) X-ROAD® Organizational Model https://x--road-global.translate.goog/X-ROAD-organizational-model?_x_tr_sl=en&_x_tr_tl=fr&_x_tr_hl=fr&_x_tr_pto=sc