AGENCE NATIONALE DES SYSTEMES D'INFORMATION DE L'ETAT

CADRE D'INTEROPÉRABILITÉ DE DJIBOUTI

Table des Matières

1 Résumé Exécutif

L'interopérabilité est la capacité de faire interagir les systèmes et les organisations. L'objectif du Cadre d'Interopérabilité de Djibouti (CID) est de définir les grands principes, les éléments constitutifs et les directives générales permettant le développement et la mise en œuvre des services électroniques pour les citoyens, les entreprises et l'administration publique.

L'interopérabilité est à la fois une condition préalable et un facilitateur de la prestation efficace des services publics. Le cadre d'interopérabilité vise à améliorer :

- la coopération entre les structures de l'administration publique en vue de mettre en place de meilleurs services rendus à ses usagers,
- le partage et la réutilisation des informations entre les structures de l'administration publique, pour accroître l'efficacité administrative et réduire la lourdeur administrative pour les citoyens et les entreprises,
- l'échange d'informations entre les acteurs de l'administration publique pour répondre aux exigences légales ou aux engagements politiques.

Le CID établit les principes d'interopérabilité à Djibouti. Les principes définissent la base et les fondements communs pour l'amélioration de l'offre des services publics. En outre, pour atteindre le paradigme d'interopérabilité par la conception *(interoperability by design)*, le CID définit un modèle qui comprend :

- quatre niveaux d'interopérabilité : juridique, organisationnel, sémantique et technique,
- une composante transversale des quatre niveaux : gouvernance intégrée du service public,
- une couche administrative en arrière-plan : la gouvernance de l'interopérabilité.

Le CID est l'accord négocié entre les organes de l'administration publique pour une approche commune d'interconnexion des systèmes d'information et des services. Le modèle conceptuel défini dans le CID doit être suivi pour construire des composants couplés à un faible degré, qui sont interconnectés sur une infrastructure partagée.

Les composants / catalyseurs les plus importants de l'infrastructure d'e-gouvernement à Djibouti sont :

- L'écosystème de services de confiance
- La plateforme d'échange de données sécurisée
- La plateforme d'identité numérique
- Le portail citoyen / Le guichet unique numérique
- Le catalogue de solutions interopérables
- L'infrastructure de données ouvertes.

2 Introduction

Dans le pilier « Bonne Gouvernance » de la stratégie à long terme « Vision Djibouti 2035 », le Président de la République, S.E.M. Ismail Omar Guelleh, promeut le renforcement des capacités de l'administration publique et de l'e-gouvernement. Comme stipulé dans la vision, une transformation profonde de l'administration devrait être basée sur : « ... le développement de l'e-gouvernance pour promouvoir la qualité des services rendus aux usagers. L'utilisation des TIC sera généralisée dans l'administration en assurant d'une part une interconnexion entre les administrations centrales elles-mêmes et leurs services déconcentrés, et d'autre part les services de l'administration seront mis en ligne et accessibles aux populations. ». Le Cadre d'Interopérabilité de Djibouti soutiendra la réalisation de 6 axes de la stratégie e-gouvernement 2020-2022[1]:

- Axe 1 : Renforcement de l'infrastructure
- Axe 2 : La création d'un cyber-environnement sécurisé
- Axe 3 : La mise en place de l'interopérabilité
- Axe 4 : Renforcement du cadre juridique
- Axe 5 : Le développement des services numériques
- Axe 6 : Renforcement des capacités des ressources humaines et institutionnelles

La République de Djibouti modernise son Administration Publique en introduisant des services publics numériques. En créant des services électroniques spécifiques au sein de l'administration, il existe un risque de multiplier des environnements numériques isolés et des barrières électroniques qui empêchent les structures de l'administration publique de coopérer et de se connecter entre elles. Pour garantir l'interconnectivité, il est nécessaire de mettre en place et d'exécuter des systèmes interopérables qui assurent une communication efficace entre les composants numériques, tels que les appareils, les réseaux et les référentiels de données. Pour cette raison, les efforts de numérisation du secteur public doivent être bien coordonnés à un niveau gouvernemental pour éviter la fragmentation numérique.

Le Cadre d'Interopérabilité de Djibouti (CID) est le guide, à travers un ensemble de recommandations sur la façon de :

- améliorer la gouvernance de leurs activités d'interopérabilité,
- établir des relations inter-organisationnelles,
- rationaliser les processus de soutien des services numériques, et
- veiller à ce que la législation existante et nouvelle ne compromettent pas les efforts d'interopérabilité.

[1] STRATÉGIE NATIONALE DE L'e-GOUVERNEMENT 2020-2022. (Document interne, 39 p)

2.1 Définitions

2.1.1 Interopérabilité

L'interopérabilité est la capacité de faire en sorte que les systèmes et les organisations fonctionnent ensemble (inter-opèrent). Dans le document suivant, le terme « interopérabilité » est utilisé au sens large, il englobe non seulement les facteurs techniques, mais également sociaux, politiques et organisationnels. Aussi, nous utilisons la définition de la Commission Européenne[2], qui a été acceptée dans le contexte gouvernemental :

"L'interopérabilité est l'aptitude d'organisations à interagir en vue de la réalisation d'objectifs communs, mutuellement avantageux, impliquant l'échange d'informations et de connaissances entre ces organisations via les processus métiers qu'elles prennent en charge, grâce à l'échange de données entre leurs systèmes informatiques."

2.1.2 Service Public

Dans ce document, nous suivons l'approche orientée service. Cela signifie que les activités de chaque organisation sont des services. Un service peut être :

- une activité répétitive, un comportement discret qu'un composant de l'organisation effectuerait sous une requête ou un déclencheur.
- un élément de comportement qui fournit des fonctionnalités spécifiques en réponse aux demandes d'acteurs ou d'autres services.

Un **service public à Djibouti** comprend tout service du secteur public fourni par des organismes de l'administration publique, soit entre eux, soit à des entreprises ou à des citoyens.

2.1.3 Cadre d'Interopérabilité de Djibouti

Le **Cadre d'Interopérabilité de Djibouti (CID)** est l'accord intergouvernemental sur la façon d'aborder la prestation de services publics de manière interopérable. Il définit des lignes directrices générales d'interopérabilité sous la forme de principes, de modèles et de recommandations communs.

Le CID s'inspire de la terminologie et de l'approche d'un cadre d'interopérabilité largement reconnu au niveau international. Par rapport à la structure du cadre cité, le CID contient un chapitre supplémentaire sur l'architecture d'interopérabilité, qui décrit les principaux composants / catalyseurs de l'infrastructure d'e-gouvernement à Djibouti :

- L'écosystème d'échange de données sécurisé

---

[2] https://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0019.02/DOC_3&format=PDF

- L'écosystème d'identification électronique et de services de confiance
- Le catalogue des solutions interopérables
- L'infrastructure de données ouvertes
- Point de contact unique

2.2 Objectif du CID

L'interopérabilité est à la fois une condition préalable et un facilitateur de la prestation efficace des services publics. Le cadre d'interopérabilité vise à améliorer :

- **la coopération** entre les acteurs de l'administration publique pour de meilleurs services publics rendus aux usagers,
- **l'échange d'informations** entre les acteurs de l'administration publique, pour répondre aux exigences légales ou aux engagements politiques,
- **le partage et la réutilisation des informations** entre les acteurs de l'administration publique, pour accroître l'efficacité administrative et réduire la lourdeur administrative des citoyens et des entreprises.

Le CID vise à :

- **réduire le coût** des services publics pour les acteurs de l'administration publique, les entreprises et les citoyens,
- **améliorer** la prestation de services publics aux citoyens et aux entreprises.

Le CID est un accord largement accepté pour les acteurs administratifs, qui se concentre sur les principes, les mécanismes et les composants, permettant des services orientés vers les usagers de l'administration - pour les employés de la fonction publique, les entreprises et les citoyens. Il peut être utilisé comme :

- un guide pour l'élaboration de concepts pour les systèmes d'information - facilitateurs d'interopérabilité - à l'échelle nationale
- un accompagnement des chefs de projets informatiques de l'administration publique pour l'élaboration des concepts des systèmes d'information de leurs établissements,
- une liste d'exigences pour les marchés publics.

Les objectifs spécifiques du CID sont de :

- faciliter la transformation de l'administration publique institutionnelle en une administration centrée sur les services, où tous les citoyens peuvent communiquer avec l'État sans connaître sa structure interne et la répartition des rôles des institutions gouvernementales,
- réduire les dépenses informatiques du secteur public grâce à des principes et solutions communs bien acceptés,

- améliorer l'interopérabilité des nouveaux projets informatiques grâce à une utilisation coordonnée des services d'infrastructure commune, fournis de façon centralisés, et des normes ouvertes,
- améliorer la coordination et la gestion des systèmes d'information de l'État et accélérer le développement des solutions informatiques,
- contribuer au co-développement du système d'information de l'Etat,
- permettre le développement autonome de tous les systèmes, dans le respect des principes d'interopérabilité organisationnelle, sémantique et technique,
- approuver la libre concurrence dans le domaine des marchés publics.

Le groupe du secteur public concerné par le CID comprend :

- les Secrétaires Généraux (SG)
- les Directeurs Généraux (DG),
- les Directeurs Financiers (DF),
- les Directeurs de la Sécurité des Systèmes d'Information (DSSI),
- les Directeurs des Systèmes d'Informations (DSI),
- les Directeurs Techniques (DT) ou les Directeurs des Opérations (DO).

De plus, il peut être utilisé comme ligne directrice pour les gestionnaires du secteur privé et les chefs de projet qui offrent des services de développement des TIC et d'administration au secteur public.

L'Agence Nationale des Systèmes d'Information de l'Etat (ANSIE), en tant qu'organisme responsable du développement coordonné du système d'information de l'État, est chargé de maintenir et d'actualiser le cadre d'interopérabilité et les documents associés. Le groupe interinstitutionnel de travail sur l'interopérabilité conseillera l'ANSIE sur l'élaboration de ces documents d'interopérabilité.

2.3 Portée du CID

Le CID est applicable à tous les acteurs de l'administration publique à Djibouti. Il définit les conditions de base pour parvenir à l'interopérabilité à tous les niveaux de l'administration. Ce document s'adresse à tous ceux impliqués dans la définition, la conception, le développement et la prestation des services publics à Djibouti.

Le CID est orienté vers le développement d'un écosystème de services publics dans lequel les propriétaires et concepteurs de systèmes et de services publics prennent conscience des exigences d'interopérabilité, et les acteurs de l'administration publique sont prêts à collaborer les uns avec les autres pour permettre un flux d'informations transparent avec les entreprises et les citoyens.

La portée du CID couvre trois types d'interaction :

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

2.4 Structure et Présentation du CID

Le contenu et la structure du CID sont présentés ci-dessous :

- Le chapitre 3 présente un ensemble de principes destinés à établir des comportements généraux en matière d'interopérabilité. Le chapitre donne un ensemble étendu d'exigences / recommandations pour l'administration djiboutienne.
- Le chapitre 4 présente un modèle d'interopérabilité, qui organise en couches les différents aspects d'interopérabilité à traiter lors de la conception des services publics.
- Le chapitre 5 présente un modèle conceptuel de services publics interopérables. Le modèle est aligné sur les principes d'interopérabilité et promeut l'idée d'« interopérabilité dès la conception ».
- Le chapitre 6 présente les concepts clés de l'architecture d'interopérabilité et encourage le développement de blocs de construction normalisés pour l'e-gouvernement de Djibouti.
- Le chapitre 7 conclut le document en donnant un aperçu et en liant les principaux éléments du CID.

Les mots clés de ce document « DEVOIR », « NE DEVOIR PAS », « OBLIGATOIRE », « RECOMMANDÉ », « POUVOIR » et « OPTIONNEL » doivent être interprété comme spécifié ci-dessous. Ceci a été adapté de la version anglaise de ce document, et a été initialement spécifié par l'Internet Engineering Task Force (IETF)[3]. Pour souligner la pertinence de ces mots, ils ont été fournis en majuscules et leurs significations sont les suivantes :

Les conclusions et exigences les plus importantes ont été fournies dans des encadrés. Ils sont numérotés en continu dans le document.

[3] Internet Engineering Task Force (IETF) RFC 2119: „Key words for use in RFCs to indicate requirements levels" (RFC 2119: Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigences): https://tools.ietf.org/html/rfc2119

3 Principes Sous-jacents

Ce chapitre énonce les principes généraux de bonne administration qui sont pertinents pour le processus de création des services publics et de mise en place des systèmes et services d'information djiboutiens. Ces principes ont été adaptés aux besoins de l'administration djiboutienne. Les principes d'interopérabilité sont des bases fondamentales pour conduire les actions d'interopérabilité.

Les douze principes sous-jacents du CID sont regroupés en quatre catégories :

- Principe définissant le contexte des actions de l'administration djiboutienne en matière d'interopérabilité (principe 1) ;
- Principes fondamentaux d'interopérabilité (principes 2 à 5) ;
- Principes liés aux besoins et attentes génériques des usagers (principes 6 à 9) ;
- Principes fondamentaux de la coopération entre les acteurs de l'administration publique (principes 10 à 12).

3.1 Principe 1 : Subsidiarité

Subsidiarité. Les décisions de politique informatique à Djibouti sont prises au plus près des institutions publiques, des entreprises et des citoyens. L'autorité centrale n'agit que si une action centrale est plus efficace qu'une action prise au niveau local. L'application des principes de subsidiarité signifie que les décisions centralisées, ayant un impact possible sur le niveau local, sont utilisées aussi rarement que possible.

Au niveau central, il est préférable de réaliser que des services d'infrastructure communs (par exemple, une infrastructure à clé publique, une plateforme d'échange de données sécurisée, un catalogue de solutions) et des systèmes fournissant aux usagers des services conjoints des institutions du secteur public (par exemple, le portail des citoyens).

Le principe de subsidiarité ne restreint pas la coopération des institutions du secteur public dans l'élaboration de solutions standard communes.

3.1. Les systèmes d'information DOIVENT respecter les structures organisationnelles et les disciplines commerciales existantes. Le réaménagement des organisations et des grandes disciplines commerciales DOIT être atteint grâce à des systèmes de liaison utilisant des services.

3.2. Toutes les institutions du secteur public DOIVENT aligner et maintenir alignés leurs cadres et stratégies sur le CID.

3.3. Les décisions politiques nationales liées aux technologies de l'information DEVRAIENT être appliquées uniquement si elles sont plus efficaces que celles prises dans les institutions du secteur public.

3.4. Au lieu de centraliser les systèmes d'information, ils DOIVENT être liés entre eux à travers les services.

3.2 Principe 2 : Ouverture

Le concept d'ouverture concerne principalement les données, les spécifications et les logiciels.

Un organisme administratif de Djibouti DEVRA être obligé de veiller à ce que les informations publiques soient publiées de manière proactive sur sa propre ressource électronique (appropriée). Les informations publiques publiées de manière proactive devront être ouvertes et également accessibles à toute personne. Il est inadmissible de facturer des frais ou d'introduire toute autre restriction à l'accès aux informations publiques publiées de manière proactive, sauf dans les cas prévus par la loi. En outre, des réformes juridiques PEUVENT être envisagées pour limiter autant que possible les restrictions légales à l'accès à l'information.

3.5. Les organismes administratifs DOIVENT publier les données, dont ils sont propriétaires, en tant que données ouvertes ou autoriser l'utilisation de services pour accéder aux données, sauf si certaines restrictions s'appliquent.

L'utilisation de technologies et de produits logiciels *open source* peut aider à réduire les coûts de développement, éviter un effet de verrouillage et permettre une adaptation rapide aux besoins commerciaux spécifiques, car les communautés de développeurs qui les prennent en charge les adaptent constamment. Les acteurs de l'administration publique DEVRAIENT non seulement utiliser des logiciels libres, mais aussi, dans la mesure du possible, contribuer aux communautés de développeurs pertinentes. L'*open source* est un catalyseur du principe sous-jacent de la réutilisabilité.

3.6. Les acteurs de l'administration publique DEVRAIENT garantir des règles du jeu équitables pour les logiciels *open source*, et démontrer une prise en compte active et équitable de l'utilisation de logiciels *open source*, compte tenu du coût total de possession de la solution.

Le niveau d'**ouverture d'une spécification / norme** est déterminant pour la réutilisation des composants logiciels mettant en œuvre cette spécification. Si le principe d'**ouverture** s'applique intégralement :

- toutes les parties prenantes pourraient contribuer à l'élaboration de la spécification et une consultation publique fait partie du processus de prise de décision,
- la spécification est disponible pour que tout le monde puisse l'étudier,

- les droits de propriété intellectuelle sur la spécification sont concédés sous licence aux conditions FRAND[4], d'une manière qui permet la mise en œuvre dans des logiciels propriétaires et *open source*,[5] et de préférence sur une base libre de redevances.

L'effet positif des spécifications ouvertes est démontré par l'écosystème Internet. Cependant, les administrations publiques PEUVENT décider d'utiliser moins de spécifications ouvertes si celles-ci n'existent pas ou ne répondent pas aux besoins fonctionnels. Dans tous les cas, les spécifications DOIVENT être matures et suffisamment soutenues par le marché, à moins qu'elles soient utilisées pour créer des solutions innovantes.

3.7. Les acteurs de l'administration publique DOIVENT privilégier les spécifications ouvertes, en tenant dûment compte de la couverture des besoins fonctionnels, de la maturité, du soutien du marché et de l'innovation.

3.3 Principe 3 : Transparence

La transparence dans le contexte du CID fait référence à :

- Permettre une visibilité à l'intérieur de l'environnement administratif d'une administration publique. Il s'agit de permettre aux usagers l'administration publique de visualiser et de comprendre les règles administratives, les processus, les données, les services et le processus décisionnel.
- Assurer la disponibilité des descriptions des interfaces des systèmes d'information. Les organismes de l'administration publique exploitent de nombreux systèmes d'information souvent hétérogènes et disparates à l'appui de leurs processus internes. L'interopérabilité dépend de la garantie de la transparence des interfaces existantes avec ces systèmes et les données qu'ils traitent. À son tour, l'interopérabilité facilite la réutilisation des services et des données, et permet à ceux-ci d'être intégrés dans des systèmes plus grands.
- Garantir le droit à la protection des données à caractère personnel, en respectant le cadre juridique applicable aux grands volumes de données à caractère personnel des citoyens, détenues et gérées par les institutions de l'administration publique.

3.8. L'administration publique DOIT assurer une visibilité interne et fournir des interfaces externes pour les services publics.

[4] FRAND : équitable, raisonnable et non discriminatoire (de l'anglais : *Fair, Reasonable And Non-Discriminatory*).

[5] Cela favorise la concurrence, car les fournisseurs travaillant sous divers modèles commerciaux peuvent se faire concurrence pour fournir des produits, des technologies et des services basés sur ces spécifications.

3.4 Principe 4 : Réutilisation

La réutilisation signifie que les organismes des administrations publiques, confrontées à un problème spécifique, cherchent à tirer parti du travail des autres en examinant ce qui est disponible, en évaluant son utilité ou sa pertinence par rapport au problème en question et, le cas échéant, en adoptant des solutions qui ont prouvé leur valeur ailleurs. Cela nécessite que l'administration publique soit ouverte au partage de ses solutions, concepts, cadres, spécifications, outils et composants d'interopérabilité avec d'autres.

La réutilisation des solutions informatiques (par exemple, les composants logiciels, les interfaces de programmation d'applications, les normes), des informations et des données, est un catalyseur de l'interopérabilité et améliore la qualité car elle étend l'utilisation opérationnelle et permet d'économiser du temps et de l'argent. Ces normes et spécifications existantes PEUVENT et DEVRAIENT être utilisées plus largement au-delà du domaine pour lequel elles ont été initialement développées.

3.9. L'administration publique DEVRAIT réutiliser et partager des solutions, et coopérer pour le développement de solutions communes.

3.10 L'administration publique DOIT réutiliser et partager les informations et les données, sauf si certaines restrictions de confidentialité s'appliquent.

3.5 Principe 5 : Neutralité Technologique et Portabilité des Données

Lors de la mise en place de systèmes et de services d'information, l'administration publique DOIT se concentrer sur les besoins fonctionnels et différer le plus longtemps possible les décisions en matière de technologie, afin d'éviter d'imposer des technologies ou des produits spécifiques à leurs partenaires et de pouvoir s'adapter à un environnement technologique en évolution rapide. L'administration publique devrait rendre l'accès aux services publics indépendant de toute technologie ou produit spécifique. La législation NE DOIT PAS prescrire des technologies spécifiques.

3.11. L'administration publique NE DEVRA PAS imposer de solutions technologiques disproportionnées spécifiques aux citoyens, aux entreprises et aux autres organes administratifs, lors de la mise en place des systèmes et des services d'information.

3.12. Lors du développement de la fonctionnalité des systèmes d'information, les décisions technologiques DOIVENT être prises le plus tard possible.

Le principe exige que les données puissent être facilement transférées entre différents systèmes pour éviter le verrouillage, pour soutenir la libre circulation des données et pour garantir des règles de jeux équitables. La portabilité des données est la capacité de déplacer et de réutiliser facilement les données entre applications et systèmes différentes.

3.13. L'administration publique DOIT veiller à ce que les données soient facilement transférables entre les systèmes et les services.

3.14. Les interfaces des systèmes d'information DOIVENT être créées de manière neutre sur le plan technologique, en utilisant des normes ouvertes, prescrites dans le CID (XML, WSDL, SOAP, etc.).

3.6 Principe 6 : Approche Centrée sur l'Utilisateur

Les utilisateurs des services publics sont tout acteur de l'administration publique, citoyen ou entreprise accédant et bénéficiant de l'utilisation de ces services. Les besoins des utilisateurs DEVRAIENT être pris en compte lors de la détermination des services publics à fournir et de la manière dont ils doivent être fournis.

Par conséquent, dans la mesure du possible, les besoins et les exigences des utilisateurs DEVRAIENT guider la conception et le développement des services publics, conformément aux attentes suivantes :

- Une approche de prestation de services **multi-canaux**, c'est-à-dire la 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 des circonstances et de leurs besoins ;
- Un point de contact unique DEVRAIT être mis à la disposition des usagers, pour masquer la complexité administrative interne et faciliter l'accès aux services publics, par ex. lorsque plusieurs organismes doivent travailler ensemble pour fournir un service public ;
- Les commentaires/*feedback* des usagers DEVRAIENT être systématiquement collectés, évalués et utilisés pour concevoir de nouveaux services publics et pour améliorer encore les services existants ;
- Dans la mesure du possible, en vertu de la législation en vigueur, les usagers devraient pouvoir fournir des données qu'une seule fois, et les organes administratifs DEVRAIENT être en mesure de récupérer et de partager ces données pour servir l'usager, conformément aux règles de protection des données ;
- Les usagers DEVRAIENT être invités à fournir uniquement **les informations nécessaires** pour obtenir un service public donné.

3.15. Un usager DEVRAIT être en mesure de choisir un type de canal de service adéquat : bureau de service, poste, téléphone, courrier électronique et autres canaux Internet.

3.16. Une personne identifiée avec une pièce d'identité électronique ou avec d'autres moyens sécurisés DOIT être en mesure de demander la prestation de tout service public électronique.

3.17. Le portail citoyen DOIT servir de point de contact unique pour les services publics. Il est RECOMMANDÉ que plusieurs organes administratifs travaillent ensemble pour fournir des services groupés via le portail citoyen.

3.18. Les commentaires/*feedback* des utilisateurs DEVRAIENT être systématiquement collectés, évalués et utilisés comme base pour une amélioration ultérieure du service. Des mécanismes pour impliquer les usagers dans l'analyse, la conception, l'évaluation et le développement ultérieur des services publics djiboutiens DEVRAIENT être mis en place.

3.19. Les données DOIVENT être fournies par les utilisateurs qu'une seule fois, et les organes administratifs DEVRAIENT être en mesure de récupérer et de partager ces données en tenant compte des règles et de la législation en matière de protection des données.

3.20. L'approche basée sur l'institution DOIT être remplacée par une approche orientée sur l'usager. Les institutions DOIVENT fournir des informations de leur propre initiative.

3.7 Principe 7 : Inclusion et Accessibilité

L'**inclusion** vise à permettre à chacun de profiter pleinement des opportunités offertes par les nouvelles technologies pour accéder et utiliser les services publics, en surmontant les fractures sociales et économiques, et l'exclusion.

L'**accessibilité** garantit que les personnes atteintes d'un handicap, 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 DOIVENT faire partie de tout le cycle de vie de développement d'un service public en termes de conception, de contenu de l'information et de livraison. Il doit être conforme aux spécifications d'e-accessibilité largement reconnues au niveau international.

L'inclusion et l'accessibilité impliquent généralement une diffusion multi-canaux. La prestation de services traditionnelle sur papier ou en personne devra 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.

3.21. L'administration publique DEVRA veiller à ce que tous les sites Web et services publics du secteur public soient accessibles à tous les citoyens, y compris les personnes atteintes d'un handicap ou ayant des besoins particuliers.

2.22. Les interfaces des systèmes d'information, des sites Web et des services du secteur public DEVRONT être conformes aux critères de qualité WCAG (*Web Content Accessibility Guidelines* - Règles pour l'accessibilité des contenus Web) - niveau AA.

3.23. Les institutions du secteur public DOIVENT fournir des informations dans des formats ouverts. Les citoyens n'ont pas à faire de dépenses supplémentaires pour utiliser les informations (par exemple, obtenir leur propre logiciel).

3.8 Principe 8 : Sécurité et Protection de la Vie Privée

Les citoyens et les entreprises DOIVENT être convaincus que lorsqu'ils interagissent avec les autorités publiques, ils le font dans un environnement sûr et digne de confiance et en pleine conformité avec les réglementations pertinentes. L'administration publique DOIT garantir la vie privée des usagers, ainsi que la confidentialité, l'authenticité, l'intégrité et la non-répudiation des informations fournies. La sécurité et la confidentialité sont abordées plus en détail dans la section 5.9.

Dans les limites de sécurité nécessaires, les citoyens et les entreprises DEVRAIENT avoir le droit de vérifier les informations que l'administration a collecté à leur sujet, et de décider si ces informations peuvent être utilisées à des fins autres que celles pour lesquelles elles ont été initialement fournies.

3.24. L'administration publique DEVRAIT définir un cadre commun de sécurité et de confidentialité, adopter une législation sur la protection des données et établir des processus pour les services publics, afin de garantir un échange de données sécurisé et fiable entre les organismes de l'administration publique et dans les interactions avec les citoyens et les entreprises.

3.25. Les systèmes d'information DOIVENT garantir la confidentialité, l'intégrité, l'authenticité, la disponibilité et la prouvabilité des données et des services.

3.26. Les citoyens DEVRAIENT être fournis par des services du secteur public dont ils peuvent vérifier et, si nécessaire, corriger les données collectées à leur sujet.

3.27. Les citoyens DEVRAIENT être fournis par des services du secteur public dont ils peuvent vérifier qui, et à quelles fins, a utilisé les données collectées à leur sujet.

3.9 Principe 9 : Multilinguisme

Le multilinguisme et la neutralité linguistique entrent en jeu non seulement au niveau des interfaces utilisateurs, mais à tous les niveaux de conception des services publics. Dans la mesure du possible, les informations DEVRAIENT être transférées dans un format indépendant de la langue, convenu entre toutes les parties concernées.

3.28. Pour les interfaces de systèmes d'information créées pour les résidents de Djibouti, la langue par défaut DOIT être le français.

3.29. Les interfaces de services DEVRAIENT être fournies en plus du français, également en arabe ou dans toute autre langue pertinente pour les utilisateurs.

3.10 Principe 10 : Simplification Administrative

Dans la mesure du possible, l'administration publique DEVRAIT chercher à rationaliser et à simplifier ses processus administratifs en les améliorant ou en éliminant ceux qui n'offrent pas de valeur ajoutée à ses usagers. La simplification administrative peut aider les entreprises et les citoyens à réduire la charge administrative liée au respect de la législation ou des obligations. De même, l'administration publique devrait mettre en place des services soutenus par des moyens électroniques, y compris leurs interactions avec d'autres acteurs de l'administration publique, les citoyens et les entreprises.

La **numérisation** des services publics devrait avoir lieu conformément aux concepts suivants:

- **numérique par défaut**, chaque fois qu'il y a lieu, 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 distribution multi-canaux et la politique «pas-de-mauvaise-porte», c'est-à-dire, que les canaux physiques et numériques coexistent.

3.30. L'administration publique DEVRAIT simplifier les processus et utiliser les canaux numériques chaque fois que cela est approprié pour la délivrance de services publics, pour répondre rapidement et avec une grande qualité aux demandes des usagers et pour réduire la lourdeur administrative pesant sur les usagers.

3.11 Principe 11 : Préservation des Informations

La législation devrait exiger que les décisions et les données soient stockées et puissent être consultées pendant une durée déterminée. Cela signifie que les dossiers et informations sous forme électronique détenus par l'administration publique, aux fins de la documentation des procédures et des décisions, doivent être préservés et convertis, si nécessaire, vers de nouveaux médias lorsque les anciens médias deviennent obsolètes. L'objectif est de garantir que les enregistrements et autres formes d'informations conservent leur lisibilité, leur fiabilité et leur intégrité, et soient accessibles aussi longtemps que nécessaire, sous réserve des dispositions relatives à la sécurité et à la confidentialité.

Pour garantir la conservation à long terme des documents électroniques et d'autres types d'informations, des formats devraient être choisis de manière à garantir leur accessibilité à long terme, y compris la préservation des signatures ou sceaux électroniques associés. À cet égard, l'utilisation de services de conservation qualifiés peut assurer la préservation à long terme des informations.

3.31. L’administration publique DOIT formuler une politique de préservation à long terme de l'information.

3.12 Principe 12 : Évaluation de l'Efficacité et de l'Efficience

L'administration publique doit veiller à ce que les solutions servent les entreprises et les citoyens de la manière la plus efficace et la plus efficiente possible, et offrent le meilleur rapport qualité-prix pour l'argent des contribuables. Il existe de nombreuses façons de mesurer la valeur apportée des services interopérables, y compris des considérations telles que le retour sur investissement, le coût total de possession, le niveau de flexibilité et d'adaptabilité, la réduction de la charge administrative, l'efficacité, la réduction des risques, la transparence, la simplification, l'amélioration des méthodes de travail, et le niveau de satisfaction des utilisateurs.

Diverses solutions technologiques DEVRAIENT être évaluées lorsqu’il s’agit d’assurer l'efficacité et l'efficience d'un service public.

3.32. Les organes administratifs DOIVENT évaluer l'efficacité et l'efficience des différentes solutions d'interopérabilité et des options technologiques en tenant compte des besoins des utilisateurs, de la proportionnalité et de l'équilibre entre les coûts et les avantages.

4 Couches d'Interopérabilité

Ce chapitre décrit un **modèle d'interopérabilité** qui est applicable à tous les services publics numériques et peut également être considéré comme faisant partie intégrante du paradigme de l'**interopérabilité dès la conception**. Il comprend :

- **quatre niveaux** d'interopérabilité: juridique, organisationnelle, sémantique et technique;
- une composante transversale des quatre niveaux, «**gouvernance intégrée des services publics**»;
- une couche en arrière-plan, «**gouvernance de l'interopérabilité**».

Ce modèle suit la terminologie et la méthodologie des standards internationaux d'interopérabilité, basées sur les meilleures pratiques. Le modèle est illustré ci-dessous :

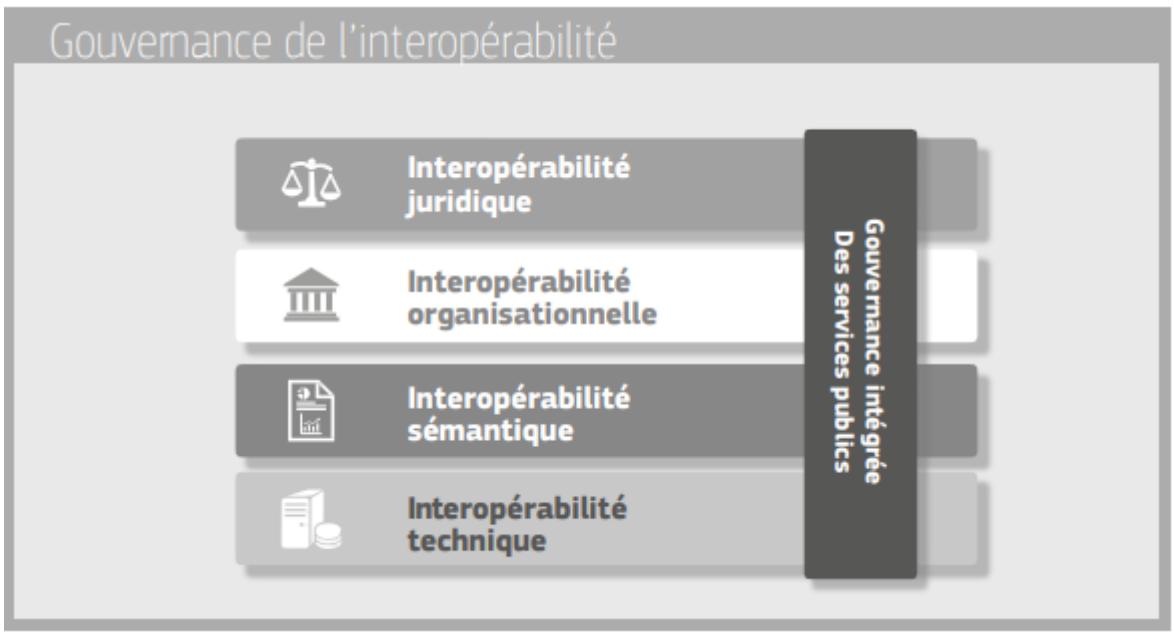

Image 1. Modèle d'interopérabilité

4.1 Gouvernance de l'Interopérabilité

4.1.1 Obstacles à la Gouvernance de l'Interopérabilité

La gouvernance de l'interopérabilité implique les décisions sur les cadres d'interopérabilité, les arrangements institutionnels, les structures, les rôles et responsabilités organisationnels, les politiques, les accords et les autres aspects liés à la mise en œuvre et au suivi de l'interopérabilité au niveau gouvernemental.

Les systèmes et services d'information à Djibouti opèrent dans un environnement **complexe et changeant**. Les efforts d'interopérabilité intersectoriels visant à faciliter la coopération entre les acteurs de l'administration publique doivent bénéficier d'un appui politique. Une interopérabilité entre les organes de l'administration publique à différents niveaux

administratifs ne pourra être mise en place que si le gouvernement accorde une priorité suffisante et affecte des ressources à leurs efforts d'interopérabilité respectifs.

Le **manque des compétences internes** constitue un autre obstacle à la mise en œuvre des politiques d'interopérabilité. L'administration publique DEVRAIT inclure des compétences d'interopérabilité dans ses stratégies d'interopérabilité, reconnaissant ainsi que l'interopérabilité est une question multidimensionnelle qui nécessite une prise de conscience et des compétences juridiques, organisationnelles, sémantiques et techniques.

La mise en œuvre des systèmes et services d'information repose souvent sur des composants communs à de nombreux propriétaires de systèmes d'information. La durabilité de ces composants DEVRAIT être assurée à plus long terme. **L'interopérabilité devrait être garantie de façon durable** et non comme un objectif ou un projet ponctuel. Étant donné que les composants communs et les accords d'interopérabilité sont le fruit des travaux menés par les organes de l'administration publique à différents niveaux (local, régional, national), la coordination et le suivi exigent d'adopter une approche holistique.

La **gouvernance de l'interopérabilité** est la clé d'une **approche globale** de l'interopérabilité, car elle rassemble tous les instruments nécessaires à son application.

4.1. L'autorité de coordination DEVRA assurer une gouvernance holistique des activités d'interopérabilité à travers les niveaux administratifs et les secteurs.

4.1.2 Gouvernance au Niveau Interagences

Une **coordination de haut niveau des activités d'e-gouvernement** entre les différentes unités du gouvernement est nécessaire. L'autorité de coordination DEVRAIT avoir la capacité juridique pour prendre des décisions contraignantes.

Toutes les institutions gouvernementales aiment moderniser leurs processus en utilisant les nouvelles technologies. L'idée de la coordination n'est pas de centraliser toutes les capacités décisionnelles et techniques mais plutôt de soutenir l'innovation et la modernisation de la prestation de services dans chaque institution gouvernementale.

Les outils de coordination sont les politiques, la législation et les réglementations, la budgétisation, le suivi, les normes communes permettant la réutilisation des données à l'échelle nationale, l'échange de données, la réutilisation des solutions logicielles et le développement rapide des services en ligne.

La coordination des investissements dans l'infrastructure et les solutions TIC est essentielle pour éviter la duplication et les surinvestissements.

Le suivi des progrès permet de comprendre l'avancement général et de l'évaluer.

4.2. Conformément aux principes de bonne gouvernance, il est RECOMMANDÉ de séparer les niveaux de prise de décision. Il est RECOMMANDÉ de conserver les décisions stratégiques, la supervision/la coordination et la mise en œuvre dans des institutions distinctes.

Il devrait y avoir des rôles, des mandats et des responsabilités clairs entre les institutions.

Le Président, L'Assemblée Nationale et le Conseil des Ministres DEVRAIENT être chargés d'approuver les principes reflétés dans le document définissant la politique d'information. Seules ces institutions peuvent garantir le soutien des changements au plus haut niveau possible avec des décisions stratégiques et suivre les progrès de la mise en œuvre.

Conseil Consultatif de la Société de l'Information : la fonction de cet organe consultatif de niveau supérieur est d'être une plate-forme de consultation pour les principales parties prenantes sur toutes les initiatives majeures et, en cas de besoin, de résoudre les litiges ou les défis de coordination au niveau politique/de haute direction. Le Conseil peut fournir des recommandations sur les questions qui ne peuvent être résolues entre les agences elles-mêmes. Le mandat officiel du Conseil devrait être de décider et superviser la stratégie et les plans d'action de l'e-gouvernement, y compris leur mise en œuvre.

4.3. Le Conseil Consultatif de la Société de l'Information DEVRAIT comprendre tous les experts clés des ministères concernés par le domaine de l'e-gouvernement, ainsi que des experts non gouvernementaux de haut niveau du pôle d'affaires, des universités et des ONG.

L'unité centrale de coordination pourrait être une agence indépendante rattachée à la Présidence de la République et DOIT avoir un mandat clair. Il est important que l'unité centrale de coordination rende compte directement à la Présidence, pour s'assurer que les décisions et les progrès auront un niveau élevé de soutien politique et de ressources disponibles.

4.4. L'Agence Nationale des Systèmes d'Information de l'État (ANSIE) tient le rôle d'unité centrale de coordination.

Les ministères, départements, autres agences et institutions publiques sont responsables de leurs propres processus opérationnels. Ils peuvent choisir et mettre en œuvre des technologies par eux-mêmes, dans le respect des principes communément acceptés.

Il est RECOMMANDÉ de centraliser l'élaboration des politiques et des normes, et de décentraliser la mise en œuvre. Cela signifie que les principes de la politique d'information et de la législation de soutien seront développés par l'unité de coordination, en impliquant les parties prenantes. Les investissements clés et autres décisions de financement à grande échelle devraient également être coordonnés dans la même unité.

Il est recommandé d'avoir un Conseil Consultatif sur les Politiques au-dessus de l'unité de coordination (comme décrit ci-dessous).

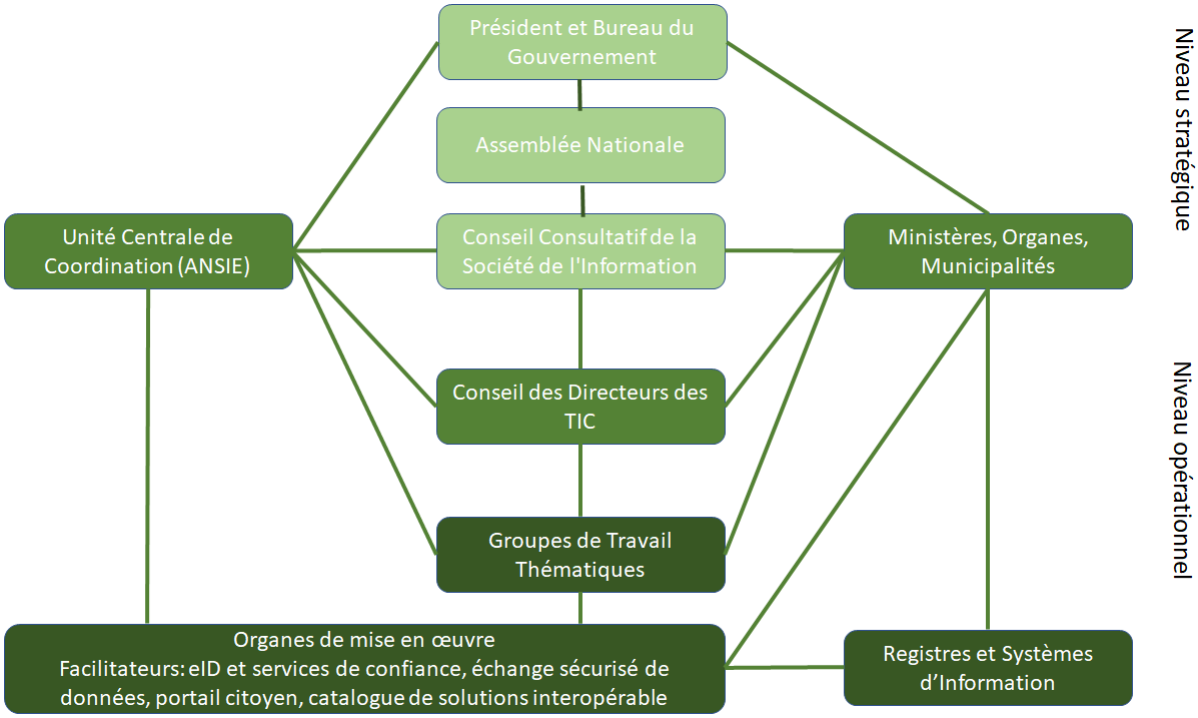

Image 2. Structure organisationnelle de l'e-gouvernance et parties prenantes au niveau interinstitutionnel

Conseil des Directeurs des TIC

Le gouvernement pourrait envisager la création du Conseil des Directeurs des TIC, en tant qu'organe de consultation, couvrant à la fois les aspects stratégiques et opérationnels. Ses membres doivent être tous les directeurs de l'information/directeurs des Systèmes d'Information/directeurs technique ou directeurs des opérations/directeurs des départements TIC des ministères/départements. En outre, certains experts extérieurs au gouvernement peuvent participer (ONG, représentants du milieu universitaire).

La tâche du Conseil est d'être le principal point de consultation sur les questions stratégiques de développement de l'e-gouvernement, avec les responsables de la mise en œuvre dans les ministères et les agences. Il permet également de créer des espaces d'échanges technologiques et de partage des bonnes pratiques. Il peut également être considéré comme un instrument permettant de consulter immédiatement les parties prenantes appropriées de l'e-gouvernement.

4.5. L'ANSIE, en tant qu'unité de coordination, DEVRAIT assurer le secrétariat et la présidence du Conseil.

Parties Prenantes

Les principales parties prenantes au niveau interinstitutionnel sont :

- **ANSIE** - Agence Nationale des Systèmes d'Information de l'Etat, Présidence la République, est responsable de la stratégie et de l'architecture de l'e-gouvernement, de la planification budgétaire de l'e-gouvernement et de la coordination des initiatives

intergouvernementales. L'ANSIE a le droit de superviser d'autres institutions gouvernementales sur la mise en œuvre des politiques et plans de sécurité numérique, de la qualité des services en ligne, entre autres.

- Ministère Délégué chargé de l'Économie Numérique et de l'Innovation
- Ministère de l'Intérieur
- Ministère du Budget
- Ministère de la Santé
- Ministère des Affaires Sociales et des Solidarités
- Ministère Chargée des Postes et des Télécoms
- Ministère du Travail chargé de la Formalisation et de la Protection Sociale
- Ministère de l'Economie et des Finances chargé de l'Industrie
- Ministère de l'Education Nationale et de la Formation Professionnelle
- Ministère de l'Enseignement Supérieur et de la Recherche
- Ministère de la Justice et des Affaires Pénitentiaires, chargé des Droits de l'Homme

Autres parties prenantes importantes :

- Universités et autres institutions de recherche et développement
- Associations du secteur des TIC
- Entreprises de logiciels et de matériel informatique
- Banques et entreprises de télécommunications
- Fournisseurs de services d'identité et de confiance numérique
- Communautés de données ouvertes
- Communautés de logiciels *open source*
- Groupes de défense des droits humains numériques
- Autres organismes communautaires

Activités, parties prenantes, donateurs, partenaires internationales

- e-Governance Academy
- Cisco
- Smart Africa
- Banque Mondiale
- Agence Française du Développement (AFD)
- Banque Africaine de Développement (BAD)
- PNUD

4.1.3 Financement

Pour un e-gouvernement durable, un financement constant doit également être assuré. Les gouvernements peuvent avoir divers modèles de financement. Nous décrivons ici les options de financement des solutions d'e-gouvernement sans inclure les infrastructures de télécommunications qui DEVRAIENT être assurées par des opérateurs privés dotés de mécanismes de financement complexes.

Le financement de l'e-gouvernement peut être décrit comme suit :

- Le gouvernement (ou les donateurs) finance, à partir du budget d'investissement, les solutions à l'échelle nationale (équipements, expertises, logiciels).
- Les frais de maintenance, assistance, développements ultérieurs, etc. sont couverts par le budget de fonctionnement de l'État.

Le retour sur investissement n'est pas directement calculé. Il va de soi que les solutions interopérables stimuleront l'économie, réduiront la corruption, assureront l'efficacité globale et sectorielles.

Il PEUT y avoir des frais de service pour la plupart des services de l'administration publique fournis à ses usagers (par ex. enregistrer le transfert de propriété des véhicules, enregistrer une nouvelle entreprise, etc.). Il est RECOMMANDÉ de maintenir le financement des coûts de fonctionnement de l'e-gouvernement à un niveau stable. Les frais de service doivent être maintenus aussi bas que possible.

4.1.4 Normes et Spécifications

Le gouvernement adopte des normes et des spécifications ouvertes pour les données et les processus technologiques du gouvernement. Les sept principes[6] qui seront utilisés pour l'adoption des normes par le gouvernement sont :

- **Partir des besoins des utilisateurs** - Les spécifications informatiques du gouvernement sont basées sur les besoins des usagers, exprimés en termes de capacités avec les normes ouvertes associées pour l'interopérabilité des logiciels, le format des données et des documents.
- **Adopter des normes ouvertes pour permettre la concurrence des fournisseurs sur un pied d'égalité** - Les normes ouvertes peuvent être mises en œuvre par un large éventail de fournisseurs, en les retenant pour les spécifications informatiques, le gouvernement supprime les obstacles à la concurrence tels que le verrouillage.
- **Les choix de normes doivent favoriser la flexibilité et le changement** - Les technologies de l'information, les données du gouvernement ainsi que les normes sur lesquelles elles reposent sont des catalyseurs de changement donnant aux services la liberté d'évoluer en fonction des besoins changeants des utilisateurs, des attentes et de l'innovation technologique.

[6] Ces principes sont adoptés de la politique de normes ouvertes du Royaume-Uni: https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles

- **Adopter des normes ouvertes qui soutiennent des coûts faibles** - Les décisions sont basées sur la solution la plus économique pour le secteur public dans son ensemble et ayant des faibles coûts.
- **Les décisions sur la sélection des normes sont bien informées** - La sélection efficace des normes pour les spécifications informatiques du gouvernement est le résultat d'une prise de décision pragmatique et éclairée, prenant en compte les conséquences pour les citoyens, les utilisateurs et les finances publiques.
- **Sélectionner les normes en utilisant des processus justes et transparents** - Le processus de sélection et d'adoption des normes ouvertes dans l'informatique est transparent, permettant l'engagement avec le public et les experts en la matière.
- **Équitable et transparente dans la spécification et la mise en œuvre des normes** - L'approvisionnement informatique du gouvernement, les spécifications, les plans de mise en œuvre et les exemptions convenues dans la politique des normes ouvertes sont ouverts et transparents.

Les principes et la structure des normes du secteur public et les normes convenues ont été décidés dans le processus de construction de la solution d'interopérabilité de Djibouti. Le secteur public convient, sous la direction du groupe de travail sur les normes ouvertes et en coopération avec d'autres parties concernées, de l'ensemble minimal de normes ouvertes du secteur public, dont la conformité est obligatoire pour le secteur public. Le choix et l'évaluation des normes sont publics et équilibrés. La liste des normes recommandées sera publiée sur le web par l'autorité de coordination et revue une fois par an.

4.6. Les organes de l'administration POURRAIENT mettre en œuvre les principes des normes ouvertes en utilisant des logiciels *open source* et propriétaires. Les principes soutiennent l'égalité d'accès aux contrats informatiques du gouvernement, et améliorent la flexibilité et la capacité lors de la coopération avec d'autres organisations gouvernementales, les citoyens et les entreprises.

4.7. Les organes de l'administration DEVRAIENT suivre un ensemble minimum convenu de normes ouvertes. Le choix et l'évaluation des normes sont publics et équilibrés. La liste des normes sera revue une fois par an.

4.2 Gouvernance Intégrée des Services Publics

La prestation de services exige souvent que différents organes de l'administration publique travaillent ensemble pour répondre aux besoins des utilisateurs finaux et fournir des **services publics de manière intégrée**. Lorsque plusieurs organisations sont impliquées, il y a un besoin de coordination et de gouvernance par l'unité centrale de coordination qui a mandat pour la planification, la mise en œuvre et l'exploitation des services. Les services DEVRAIENT être régis pour assurer l'intégration, l'exécution transparente, la réutilisation des services et des données, et le développement de nouveaux services et d'« **éléments constitutifs** ».[7]

[7] Un « élément constitutif » est une unité autonome, interopérable et remplaçable encapsulant une structure interne.

4.2.1 Gouvernance au Niveau Administrative

En se concentrant ici sur la partie gouvernance, cela DEVRAIT couvrir les couches juridiques, organisationnelles, sémantiques et techniques. Assurer l'interopérabilité lors de la préparation des instruments juridiques, des processus d'organisation des affaires, de l'échange d'informations, des services et des composants qui soutiennent les services publics, est une tâche continue. En effet, l'interopérabilité est régulièrement affectée par des changements, à savoir dans la législation, les besoins des structures organisationnelles des organes de l'administration publique, les processus d'affaires, et par l'émergence de nouvelles technologies. Cela nécessite, entre autres, des structures organisationnelles, des rôles et des responsabilités pour la prestation et le fonctionnement des services publics, des accords de niveau de service, l'établissement et la gestion d'accords d'interopérabilité, des procédures de gestion du changement et des plans de continuité des activités et de qualité des données.

La gouvernance intégrée des services publics DEVRAIT inclure au minimum :

- la définition des structures organisationnelles, des rôles & responsabilités et du processus de prise de décision pour les parties prenantes impliquées;
- l'imposition d'exigences pour:
  - les aspects de l'interopérabilité, y compris la qualité, l'évolutivité et la disponibilité des éléments constitutifs réutilisables, y compris les sources d'information (registres de base, portails de données ouvertes, etc.) et d'autres services interconnectés;
  - informations/services externes, traduits en accords de niveau de service clairs (y compris sur l'interopérabilité);
- un plan de conduite du changement, pour définir les procédures et processus nécessaires pour gérer et maîtriser les changements;
- un plan de continuité d'activité/de reprise d'activité pour garantir que les services publics numériques et leurs composantes continuent de fonctionner dans diverses situations, par ex. les cyberattaques ou la défaillance des éléments constitutifs.

4.8. Les organes administratifs DEVRAIENT assurer l'interopérabilité et la coordination dans le temps lorsqu'ils exploitent et fournissent des services publics intégrés en mettant en place la structure de gouvernance nécessaire.

4.2.2 Accords d'Interopérabilité

Les organisations impliquées dans la prestation de services publics devraient conclure des **accords formels** de coopération par le biais d'**accords d'interopérabilité**. La mise en place et la gestion de ces conventions font partie de la gouvernance du service public.

Les accords doivent être suffisamment détaillés pour atteindre leur objectif, à savoir fournir des services publics, tout en laissant à chaque organisation le maximum d'autonomie possible.

Aux niveaux sémantique et technique, mais aussi dans certains cas au niveau organisationnel, les accords d'interopérabilité incluent généralement des normes et des spécifications. Sur le plan juridique, les accords d'interopérabilité sont rendus spécifiques et contraignants par la législation djiboutienne ou par des accords bilatéraux et multilatéraux.

D’autres types d’accords peuvent compléter les accords d’interopérabilité, traitant de questions opérationnelles (par exemple les mémorandums d’entente, les accords de niveau de service, les procédures des différents niveaux de support et les coordonnées, faisant référence, si nécessaire, aux accords sous-jacents aux niveaux sémantique et technique).

Étant donné que la prestation d'un service public est le résultat d'un travail collectif avec les parties qui produisent ou consomment des services, il est essentiel d'inclure des processus de conduite du changement appropriés dans les accords d'interopérabilité pour assurer l'exactitude, la fiabilité, la continuité et l'évolution du service fourni aux autres organes de l'administration publique, aux entreprises et aux citoyens.

4.9. L'administration publique DEVRAIT établir des accords d'interopérabilité à tous les niveaux, complétés par des accords opérationnels et des procédures de conduite du changement.

4.3 Interopérabilité Juridique

Chaque organe de l'administration publique contribuant à la fourniture d'un service public travaille dans le cadre juridique national. L'interopérabilité juridique consiste à garantir que les organisations opérant sous différents cadres juridiques, politiques et stratégies sont capables de travailler ensemble. Cela POURRAIT exiger que la législation ne bloque pas la mise en place de services publics et qu'il existe des accords clairs sur la façon de traiter les spécificités dans la législation, incluant la possibilité de mettre en place une nouvelle législation.

La première étape vers le traitement de l'interopérabilité juridique consiste à effectuer des « contrôles d’interopérabilité » en passant au crible la législation existante pour identifier les obstacles à l’interopérabilité : restrictions sectorielles ou géographiques. Ceci DEVRAIT vérifier l'utilisation et le stockage des données, les modèles de licence de données différents et plus élargis, les obligations trop restrictives d'utiliser des technologies numériques ou des modes de livraison spécifiques pour fournir des services publics, des exigences contradictoires pour des processus métiers identiques ou similaires, des besoins obsolètes en matière de sécurité et de protection des données, etc.

La cohérence des législations, en vue d'assurer l'interopérabilité, DEVRAIT être évaluée avant l'adoption, et en suivant régulièrement leurs performances une fois qu'elles sont mises en application.

4.10. L'administration DEVRAIT s'assurer que la législation est examinée au moyen des « contrôles d’interopérabilité », afin d'identifier tout obstacle à l'interopérabilité.

Gardant à l'esprit que les services publics djiboutiens sont clairement destinés à être fournis - entre autres - à partir des canaux numériques, les TIC doivent être prises en compte le plus tôt possible dans le processus d’élaboration des textes juridiques.

La législation proposée devrait subir un « **contrôle numérique** » :

- pour s'assurer qu'elle s'adapte non seulement au monde physique mais aussi au monde numérique (par exemple Internet) ;
- pour identifier les éventuelles barrières aux échanges numériques ;
- pour identifier et évaluer son impact TIC sur les parties prenantes.

Cela facilitera également l'interopérabilité entre les services publics à des niveaux inférieurs (sémantiques et techniques) et augmentera le potentiel de réutilisation des solutions TIC existantes, réduisant ainsi les coûts et le temps de mise en œuvre.

4.11. Lors de la rédaction d'un texte juridique visant à établir un service public, cherchant à la rendre conforme à la législation pertinente, les organes administratifs DOIVENT effectuer un « contrôle numérique » et prendre en compte les exigences en matière de protection des données.

Les domaines informatiques dans lesquels une nouvelle législation doit être créée et la législation existante doit être complétée et/ou améliorée sont énumérés ci-dessous.

Code Civil

Le Code Civil[8] comprend la plupart des questions liées aux actes administratifs, aux contrats et à la procédure civile. Le Code civil comprend des règles sur les signatures et documents électroniques. Celles-ci stipulent qu'un document électronique (écrit, sans conditions particulières sur ce qu'est un document) a la même valeur qu'un document papier à condition que la personne qui l'a signé puisse être identifiée et que le document puisse être conservé de manière à garantir son intégrité.

Télécommunication

L'objectif de la législation dans ce domaine est de créer les conditions nécessaires au développement des communications électroniques. La loi énonce les exigences relatives aux réseaux et services publics de communications électroniques, aux communications radio, à la gestion des fréquences radio et à la numération, à l'équipement et à la surveillance du respect de ces exigences et à la responsabilité en cas de violation de ces exigences.

Droit en vigueur : Loi N° 80/AN/14/7ème L portant approbation du Schéma Stratégique Intégré (SSI) du secteur des Technologies de l'Information et de la Communication (TIC) en République de Djibouti.[9]

Cybersécurité et Cybercriminalité

[8] https://www.presidence.dj/AnnexeTextes/Annexe5ad3535c167d020180415032756.pdf

[9] https://www.presidence.dj/texte.php?ID=80&ID2=2015-02-25&ID3=Loi&ID4=4&ID5=2015-02-28&ID6=n

Les concepts de cybersécurité et cybercriminalité et les méthodes de contrôle et de protection des attaques des plateformes électroniques.

Droit en vigueur : Loi N° 66/AN/14/7ème L relative au cyber sécurité et à la lutte contre la cybercriminalité.[10]

Informations du secteur public

La législation garantit que le public et tout le monde a accès aux informations destinées à un usage général, et crée pour le public des mécanismes de contrôle sur l'accomplissement des devoirs publics.

Signature numérique et infrastructure PKI

La législation précise les modalités d'utilisation d'une signature numérique et d'une procédure de surveillance des services de certification et d'horodatage.

Protection des données personnelles

La législation stipule les droits et libertés fondamentaux d'une personne conformément à l'intérêt public, lorsque ses données personnelles sont traitées.

Marchés publics

La législation stipule la procédure des marchés publics, les droits et obligations des sujets qui participent aux marchés publics ainsi que les violations de la loi, et la procédure de surveillance de l'État dans le but de promouvoir la concurrence et d'assurer la transparence des marchés publics et l'égalité de traitement des participants à la procédure d'appel d'offres.

Droit en vigueur : Loi n° 53/AN/09/6ème L Portant nouveau Code des Marchés Publics

Règlement sur l'échange de données

Le règlement, de préférence pas la loi, fixe des exigences pour la couche d'échange de données des systèmes d'information, son utilisation et sa gestion.

Gestion des registres et des systèmes d'information

L'objectif de la législation dans ce domaine est d'assurer la transparence de la gestion du système d'information de l'État, de planifier la gestion de l'information de l'État et de soutenir l'interopérabilité des bases de données de l'État, des collectivités locales et des personnes privées exerçant des fonctions publiques.

Archivage

[10] https://www.presidence.dj/texte.php?ID=66&ID2=2014-07-20&ID3=Loi&ID4=1&ID5=2014-07-31&ID6=sp

La législation en la matière prévoit la collecte, l'évaluation, la conservation et l'organisation de l'accès aux documents d'archives (y compris numériques) et les fondements du fonctionnement des archives (y compris les archives numériques).

Droit en vigueur : Loi N ° 132/AN/11/6ème L portant sur les Archives

Stratégie nationale d'e-gouvernement

La stratégie et le plan d'action correspondant seront établis pour une durée de deux ans.

Cadre d'interopérabilité

Le cadre d'interopérabilité peut être établi sous la forme d'une « législation non contraignante », par exemple sous la forme d'un décret ou d'une autre forme de réglementation.

4.12. Les systèmes d'information sont coordonnés avec les actes juridiques, d'abord, dans la dimension organisationnelle. Dans la dimension sémantique et technique, l'interopérabilité est régulée par divers accords, normes ou recommandations.

4.4 Interopérabilité Organisationnelle

Il s'agit de la manière dont les organes de l'administration publique alignent leurs processus métier, leurs responsabilités et leurs attentes pour atteindre des objectifs communs et mutuellement avantageux. En pratique, l'interopérabilité organisationnelle implique à documenter et intégrer ou harmoniser les processus métier et les informations pertinentes échangées. L'interopérabilité organisationnelle vise également à répondre aux exigences de la communauté des utilisateurs en rendant les services disponibles, facilement identifiables, accessibles et centrés sur l'utilisateur.

4.4.1 Harmonisation des Processus Métier

Pour permettre à différentes entités administratives de collaborer efficacement en vue de fournir des services publics, ils peuvent avoir besoin d'aligner leurs processus métier existants ou d'en définir et d'en établir de nouveaux.

L'harmonisation des processus métier implique de documenter ces derniers, de façon concertée et selon des techniques de modélisation communément acceptées, y compris en ce qui concerne les informations échangées, afin que tous les organes de l'administration publique contribuant à la prestation de services publics puissent comprendre le processus métier global et le rôle qu'elles y jouent.

4.13. Les administrations DEVRAIENT documenter les processus métier en utilisant des techniques de modélisation communément acceptées et convenir de la manière dont ces processus DEVRAIENT être harmonisés pour fournir un service public.

4.4.2 Relations Organisationnelles

L'approche orientée service, sur laquelle est construit le modèle conceptuel pour les services publics, implique une définition claire de la relation entre les prestataires des services et leurs utilisateurs.

Il faut trouver pour cela les instruments nécessaires à la formalisation de l'assistance mutuelle, de l'action conjointe et des processus métier interconnectés en relation avec la prestation d'un service, par ex. protocoles d'entente et accords de service entre les organes de l'administration publique.

4.14. Les administrations DEVRAIENT clarifier et formaliser les relations organisationnelles pour l'établissement et le fonctionnement des services publics.

4.5 Interopérabilité Sémantique

L'interopérabilité sémantique garantit que le format et le sens précis des données et informations échangées sont préservés et compris dans les échanges entre les parties, autrement dit que « ce qui est envoyé est ce qui est compris ». Dans le CID, l'interopérabilité sémantique couvre à la fois les aspects sémantiques et syntaxiques.

- l'aspect **sémantique** concerne le sens des éléments de données et les relations entre ces éléments. Il suppose également la mise au point de vocabulaires et de schémas spécifiques qui serviront à décrire les échanges de données, et permet que les éléments de données soient compris de la même façon par toutes les parties concernées ;
- l'aspect **syntaxique** consiste à définir le format exact des informations à échanger en termes de grammaire et de format.

Un point de départ pour améliorer l'interopérabilité sémantique est de **considérer les données et les informations comme un actif public précieux**.

4.15. L'administration publique DEVRAIT percevoir les données et les informations comme un bien public qui DEVRAIT être généré, collecté, géré, partagé, protégé et préservé de manière appropriée.

Une stratégie de gestion de l'information DEVRAIT être élaborée et coordonnée au niveau le plus élevé possible pour éviter la fragmentation et fixer des priorités.

Par exemple, les accords sur des données de référence sous forme de taxonomies, de vocabulaires contrôlés, de thésaurus, de listes de codes et de structures/modèles de données réutilisables sont des conditions préalables essentielles à l'interopérabilité sémantique. Des approches telles que la **conception fondée sur les données**, associées à des technologies de **données liées**, sont des moyens novateurs d'améliorer sensiblement l'interopérabilité sémantique.

4.16. Une stratégie de gestion de l'information DEVRAIT être mise en place au plus haut niveau possible pour éviter la fragmentation et la duplication. La gestion des métadonnées, et des données de référence DEVRAIT être prioritaire.

Des normes et des spécifications d'information solides, cohérentes et universellement applicables sont nécessaires pour permettre un échange d'informations significatif entre les organisations publiques.

4.6 Interopérabilité Technique

L'interopérabilité technique couvre les applications et les infrastructures reliant entre eux les systèmes et les services. Elle concerne notamment les spécifications d'interface, les services d'interconnexion, les services d'intégration des données, la présentation et l'échange des données et les protocoles de communication sécurisés.

Les systèmes vieillissants constituent un obstacle majeur à l'interopérabilité. Historiquement, les applications et les systèmes d'information des administrations publiques ont été développés de manière ascendante, pour essayer de résoudre des problèmes locaux et spécifiques à un domaine. Il en résulte des îlots de TIC fragmentés dont il est difficile d'assurer l'interopérabilité.

En raison de la taille des administrations publiques et de la fragmentation des solutions TIC, la pléthore de systèmes vieillissants crée un obstacle supplémentaire à l'interopérabilité au niveau technique.

L'interopérabilité technique doit être assurée, si possible, par l'utilisation de spécifications techniques formelles.

4.17. L'administration publique DEVRAIT utiliser des spécifications ouvertes, lorsqu'elles sont disponibles, pour assurer l'interopérabilité technique lors de l'établissement de services publics.

5 Modèle Conceptuel pour la Prestation de Services Publics Intégrée

5.1 Introduction

Ce chapitre propose un modèle conceptuel de services publics intégrés. Il est pertinent à tous les niveaux de gouvernance : local, structures gouvernementales, ministériel et national. Le modèle est modulaire et comprend des composants de service faiblement couplés interconnectés via une infrastructure partagée. La terminologie et l'idée principale du modèle de Djibouti intègrent les meilleures pratiques et standards internationaux. Le modèle est ajusté aux besoins de Djibouti.

5.1. L'administration publique DEVRAIT utiliser le modèle conceptuel des services publics pour créer de nouveaux services ou réorganiser les services existants et réutiliser, dans la mesure du possible, les composants de service et de données existants.

Les organes de l'administration publique doivent définir, négocier et s'accorder sur une approche commune pour l'interconnexion des composants de service. Cela doit être fait à différents niveaux de l'administration en fonction de la configuration organisationnelle. Les limites d'accès aux services et aux informations DOIVENT être définies au moyen d'interfaces et de conditions d'accès.

Il existe pour ce faire des solutions techniques reconnues et largement utilisées, comme les services web, mais leur implémentation au niveau de l'État exige des efforts concertés des organes de l'administration publique, notamment en termes de modèles, normes et accords communs ou compatibles relatifs à une infrastructure commune.

5.2. L'administration publique DOIT décider d'un schéma commun d'interconnexion des composants de service faiblement couplés et mettre en place et maintenir l'infrastructure nécessaire pour établir et maintenir les services publics au niveau de l'État.

5.2 Vue d'Ensemble du Modèle

Le modèle conceptuel favorise l'idée de l'**interopérabilité dès la conception**. Cela signifie que pour que les services publics soient interopérables, ils doivent être conçus conformément au modèle proposé et en tenant compte de certaines exigences en matière d'interopérabilité et de réutilisabilité. Le modèle promeut la réutilisabilité en tant que moteur de l'interopérabilité. Les services publics devraient réutiliser les informations et les services qui existent déjà et qui sont susceptibles d'être disponibles auprès de diverses sources à l'intérieur ou au-delà du périmètre de l'administration publique. Les informations et les services devraient être consultables et être mis à disposition dans des formats interopérables.

Les éléments de base du modèle conceptuel sont présentés ci-dessous :

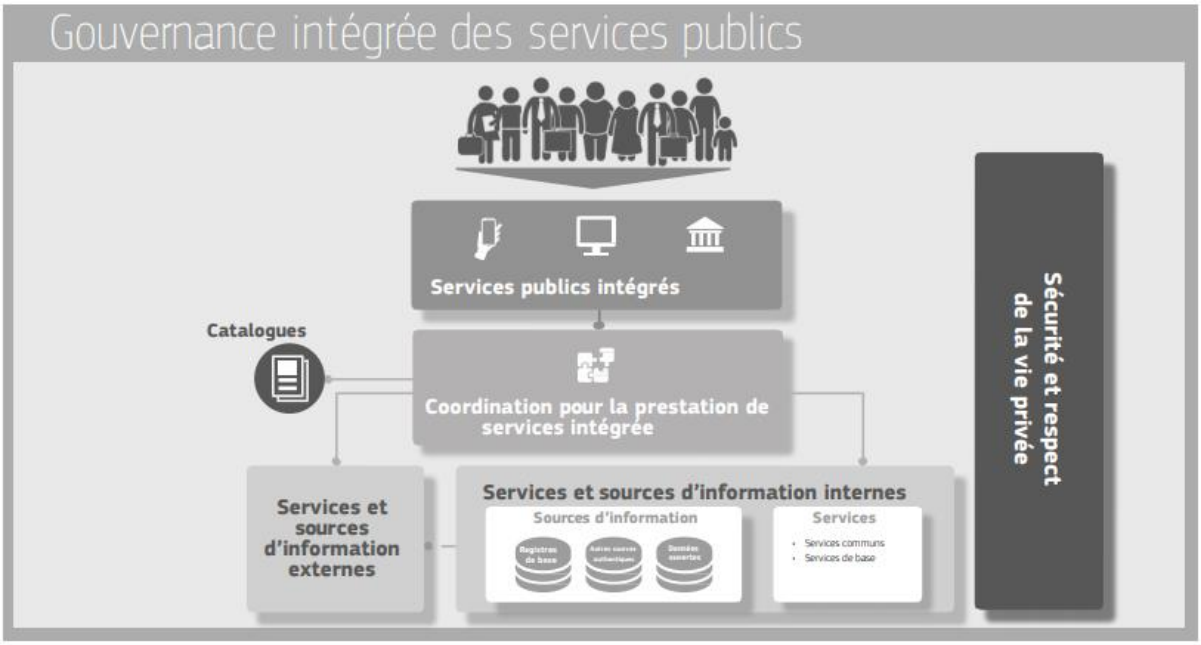

Image 3. Modèle conceptuel pour des services publics intégrés

La structure du modèle comprend :

- une «prestation de services intégrée» fondée sur une «fonction de coordination» visant à éliminer la complexité pour l'utilisateur final ;
- une politique de prestation de services «pas-de-mauvaise-porte», en proposant d'autres options et canaux pour la prestation de services, tout en assurant la disponibilité des canaux numériques (numérique par défaut) ;
- la réutilisation des données et des services pour réduire les coûts et améliorer la qualité des services et l'interopérabilité ;
- des catalogues décrivant les services réutilisables et d'autres actifs afin d'accroître leur trouvabilité et leur utilisation ;
- une gouvernance intégrée des services publics ;
- la sécurité et la protection de la vie privée.

5.3 Fonction de Coordination

La fonction de coordination assure la définition des besoins ainsi que le recours aux services appropriés et leur orchestration en vue de fournir un service public. Cette fonction doit sélectionner les sources et les services appropriés et les intégrer. La coordination peut être automatisée ou manuelle.

Les phases de processus suivantes font partie de la « prestation de services publics intégrée » et sont exécutées par la fonction de coordination.

- **Identification des besoins** : elle est déclenchée par une demande de service public par un citoyen ou une entreprise.

- **Planification** : elle suppose d'identifier les services et les sources d'information nécessaires, d'utiliser les catalogues disponibles et de les regrouper en un seul processus, en tenant compte des besoins spécifiques des utilisateurs (par exemple, la personnalisation).
- **Exécution** : elle suppose la collecte et l'échange d'informations, l'application de règles opérationnelles (conformément à la législation et aux politiques applicables) pour accorder ou refuser l'accès à un service et enfin la fourniture du service demandé aux citoyens ou aux entreprises.
- **Évaluation** : après la prestation des services, les commentaires des utilisateurs sont recueillis et évalués.

5.4 Sources et Services d'Information Internes

Les organes de l'administration publique produisent et mettent à disposition un nombre important de services, tout en conservant et en gérant un grand nombre et une grande variété de sources d'information. Ces sources d'information sont souvent inconnues en dehors d'une administration particulière (et parfois même au sein de celle-ci). Il en résulte une duplication des efforts et une sous-exploitation des ressources et des solutions disponibles.

Les **sources d'information** (registres de base, portails de données ouvertes et autres sources d'information faisant autorité) et les services disponibles non seulement à l'intérieur de l'administration publique mais aussi dans l'environnement externe peuvent être utilisés pour créer des services publics intégrés en tant que modules.

Les **modules** (sources et services d'information) devraient rendre leurs données ou leurs fonctionnalités accessibles en adoptant des approches axées sur les services.

5.3. Développer une infrastructure partagée de services réutilisables et de sources d'information qui PEUVENT être utilisées par tous les organes de l'administration publique.

Les organes de l'administration publique DEVRAIENT promouvoir des politiques de partage des services et des sources d'information de trois manières principales :

- **Réutilisation :** Lors de la conception de nouveaux services ou de l'actualisation de services existants, la première étape devrait consister à examiner si les sources d'information et les services existants peuvent être réutilisés ;
- **Publication :** Lors de la conception de nouveaux services et sources d'information ou de l'actualisation de services et sources d'information existants, les services et les sources d'information réutilisables devraient être mis à la disposition de tiers en vue d'être réutilisés ;
- **Agrégation :** Une fois que les services et les sources d'information appropriés ont été identifiés, ils devraient être groupés pour former un processus de prestation de services intégrée. Les modules devraient être combinables (« interopérabilité dès la conception ») afin de pouvoir être intégrés dans différents environnements avec une personnalisation minimale. Cette agrégation est applicable aux informations, aux services et aux autres solutions d'interopérabilité (par exemple, les logiciels).

L'approche par **bloc de construction** réutilisable trouve une application appropriée en mettant en correspondance les solutions avec les blocs de construction conceptuels d'une **architecture de référence**[11]. Ladite architecture de référence permet de détecter les composants réutilisables favorisant ainsi la rationalisation. Le résultat de cet exercice est une **cartographie**[12] de solutions, y compris leurs modules, qui PEUT être réutilisée pour répondre aux besoins opérationnels communs et assurer l'interopérabilité.

Plus précisément, pour éviter les duplications d'efforts, les coûts supplémentaires et les problèmes d'interopérabilité, tout en augmentant la qualité des services proposés, le modèle conceptuel comporte deux types de réutilisation.

- **Réutilisation des services** : différents types de services peuvent être réutilisés. Par exemple, des services publics de base tels que la délivrance d'un certificat de naissance ou des services partagés comme l'identification électronique et la signature électronique. Les services partagés peuvent être fournis par le secteur public, le secteur privé ou des partenariats public-privé ;
- **Réutilisation des informations** : les organismes de l'administration publique stockent de grandes quantités d'informations susceptibles d'être réutilisées. Par exemple : les données de référence des registres de base, en tant que données faisant autorité, utilisées par différents systèmes et applications ; les données ouvertes sous licence d'utilisation ouverte publiées par des organes publics ; d'autres types de données faisant autorité validées et gérées sous l'égide des pouvoirs publics. Les registres de base et les données ouvertes sont examinés plus en détail dans la section suivante.

5.5 Registres de Base

Les registres de base sont la pierre angulaire de la prestation de services publics. Un registre de base est une source fiable et faisant autorité d'informations qui PEUVENT et DEVRAIENT être réutilisées numériquement par des tiers, une organisation donnée étant responsable de la collecte, de l'utilisation, de la mise à jour et de la préservation des informations. Les registres de base sont des sources fiables d'informations de base sur des éléments tels que les personnes, les entreprises, les véhicules, les licences, les constructions, les lieux et les routes. Les informations de ce type constituent les « **données de référence** » pour les administrations publiques et la prestation de services publics. « Faisant autorité » signifie ici qu'un registre de base est considéré comme la « source » de l'information, c'est-à-dire qu'il représente l'état correct, est à jour et est de la plus haute qualité et intégrité possibles.

Dans le cas des registres centralisés, une entité organisationnelle unique est responsable de la qualité des données et de l'existence de mesures garantissant l'exactitude des données. Ces registres sont sous le contrôle juridique des organes de l'administration publique, tandis que leur exploitation et leur maintenance PEUVENT être externalisées si nécessaire. Il existe plusieurs types de registres de base, notamment pour des domaines tels que la population, les entreprises, les véhicules ou le cadastre. Pour les administrations, il est important de

[11] Il est RECOMMANDÉ de développer un document d'architecture d'interopérabilité pour Djibouti

[12] Les idées de la cartographie européenne PEUVENT être utilisées : https://ec.europa.eu/isa2/solutions/eira_en

disposer d'un aperçu de haut niveau du fonctionnement des registres de base et des données qu'ils stockent (un registre des registres).

Dans le cas de registres distribués, une seule entité organisationnelle DOIT être responsable de chaque partie du registre. En outre, une entité unique DOIT être responsable de la coordination de toutes les parties du registre distribué.

Le **cadre d'un registre de base** décrit les accords et l'infrastructure d'exploitation des registres de base et les relations avec les autres entités.

L'accès aux registres de base doit être réglementé pour se conformer à la confidentialité et aux autres réglementations ; les registres de base sont régis par les principes de la gérance de l'information.

Le **gérant de l'information** est l'organe (ou éventuellement la personne) responsable de la collecte, de l'utilisation, de la mise à jour, du maintien et de la suppression des informations. Ces tâches consistent notamment à définir les limites de l'utilisation de l'information, à respecter les règles de confidentialité et les politiques de sécurité, à actualiser les informations et à garantir l'accessibilité des données par les utilisateurs autorisés.

Les registres de base DEVRAIENT élaborer et mettre en œuvre un **plan d'assurance de la qualité des données** afin de garantir la qualité de leurs données. Les citoyens et les entreprises DEVRAIENT être en mesure de vérifier la précision, l'exactitude et le caractère exhaustif des données les concernant, contenues dans les registres de base.

Un guide terminologique et/ou un glossaire des termes utilisés dans chaque registre de base DEVRAIT être mis à disposition ; ils DEVRAIENT être lisibles tant par la machine que par l'Homme.

5.4. L'administration publique DEVRA mettre à la disposition des autres les sources d'information faisant autorité, tout en mettant en œuvre des mécanismes d'accès et de contrôle pour assurer la sécurité et la confidentialité conformément à la législation pertinente.

5.5. Les organes de l'administration publique DEVRONT développer des interfaces avec les registres de base et les sources d'information faisant autorité, publier les moyens sémantiques et techniques et la documentation nécessaires pour que les autres puissent se connecter et réutiliser les informations disponibles.

5.6. Les organes de l'administration publique DEVRONT associer à chaque registre de base les métadonnées appropriées, y compris la description de son contenu, l'assurance de service et les responsabilités, le type de données de référence qu'il stocke, les conditions d'accès et les licences pertinentes, la terminologie, un glossaire et des informations sur les données de référence utilisées par d'autres registres de base.

5.7. Les organes de l'administration publique DEVRONT créer et suivre des plans d'assurance de la qualité des données pour les registres de base et les données de référence connexes.

Les principaux registres de base à Djibouti sont :

- **Registre de la population.** Responsable : Bureau d'état civil / Mairie de Djibouti.
- **Registre des documents d'identité.** Responsable : Direction général de la population et de la famille (DGPF)
- **Registre des entreprises**. Responsable : Office Djiboutien de la Propriété Industrielle et Commerciale (ODPIC)
- **Registre du cadastre.** Responsable : Direction de Domaine et de la conservation foncière / Agence de Réhabilitation Urbaine et du Logement Social (ARULOS)
- **Registre de la sécurité sociale**. Responsable : Caisse nationale de sécurité social (CNSS)
- **Registre des dossiers de santé.** Responsable : Ministère de la sante
- **Registre des véhicules.** Responsable : Direction des mines et de la sécurité routière
- **Registre des textes juridiques.** Responsable : Secrétaire General du Gouvernement

5.6 Données Ouvertes

L'accent mis sur la politique de données ouvertes est matérialisé par la publication de données **lisibles par machine** à des fins d'utilisation par des tiers en vue de favoriser la transparence, la concurrence loyale, l'innovation et une **économie fondée sur les données**. En vue d'assurer des conditions équitables, l'ouverture et la réutilisation des données doivent être non discriminatoires, ce qui signifie que les données doivent être interopérables afin de pouvoir être trouvées, découvertes et traitées.

5.8. Les organes de l'administration publique DEVRAIENT établir des procédures et des processus pour intégrer l'ouverture des données dans leurs processus métier communs, procédures de travail et dans le développement de nouveaux systèmes d'information.

Il existe actuellement de nombreux obstacles à l'utilisation des données ouvertes. Elles sont souvent publiées dans différents formats ou dans des formats qui empêchent de les utiliser facilement, les métadonnées pertinentes peuvent en être absentes, les données elles-mêmes peuvent être de faible qualité, etc. Idéalement, les métadonnées de base et les sémantiques des ensembles de données ouverts DEVRAIENT être décrites dans un format standard lisible par les machines.

5.9. Les organes de l'administration publique DEVRONT publier les données ouvertes dans des formats non-propriétaires lisibles par machine. Ils DEVRONT s'assurer que les données ouvertes soient accompagnées de métadonnées de haute qualité et lisibles par machine dans des formats non-propriétaires, y compris une description de leur contenu, la façon dont les données sont collectées et leur niveau de qualité ainsi que la licence sous laquelle elles sont mises à disposition. L'utilisation de vocabulaires communs pour exprimer les métadonnées est RECOMMANDÉE.

Les données PEUVENT être utilisées de différentes façons et à des fins diverses, et la publication de données ouvertes DEVRAIT permettre cette diversité. Néanmoins, certains ensembles de données peuvent poser des problèmes aux utilisateurs, ou ces derniers

pourraient exprimer des réserves quant à leur qualité ou préférer d'autres méthodes de publication. Les commentaires collectés peuvent permettre d'en apprendre davantage sur la manière dont les ensembles de données sont utilisés et sur la façon d'améliorer leur publication.

Pour que la réutilisation des données ouvertes atteigne son plein potentiel, le caractère légal de l'interopérabilité et la sécurité juridique sont essentiels. C'est pourquoi le droit de réutiliser des données ouvertes doit être clairement communiqué dans toute l'administration et les régimes juridiques visant à faciliter la réutilisation des données, tels que les licences, devraient, dans la mesure du possible, être encouragés et standardisés.

5.10. L'administration publique DEVRAIT communiquer clairement le droit d'accès et de réutilisation des données ouvertes. Les régimes juridiques visant à faciliter l'accès et la réutilisation, tels que les licences, DEVRAIENT être normalisés autant que possible.

5.7 Catalogues

Les catalogues aident à trouver des ressources réutilisables (par exemple des services, des données, des logiciels ou des modèles de données). Il existe différents types de catalogues, par exemple des répertoires de services, des bibliothèques de composants logiciels, des portails de données ouvertes, des registres de registres de base, des catalogues de métadonnées ou encore des catalogues de normes, spécifications et directives. Des descriptions communément admises des services, des données, des registres et des solutions interopérables publiées dans les catalogues sont nécessaires pour permettre l'interopérabilité entre catalogues.

5.11. L'unité de coordination DEVRAIT mettre en place des catalogues de services publics, de données publiques et de solutions d'interopérabilité et utiliser des modèles communs pour les décrire.

5.8 Sources et Services d'Information Externes

Les organes de l'administration publique sont à amener à exploiter des services fournis en dehors de leurs périmètres par des tiers, tels que les services de paiement fournis par des établissements financiers ou les services de connectivité fournis par des fournisseurs de télécommunications. Elles ont également besoin de recourir à des sources d'information externes telles que des données ouvertes et des données provenant d'organisations internationales, de chambres de commerce, etc. De plus, des données utiles peuvent être recueillies par l'intermédiaire de l'Internet des objets (capteurs, par exemple) et des réseaux sociaux.

5.12. Lorsque c'est possible et utile, des sources et des services d'information externes DEVRAIENT être utilisés lors du développement des services publics.

5.9 Sécurité et Protection de la Vie Privée

La sécurité et la protection de la vie privée sont des préoccupations essentielles dans la prestation de services publics. Les administrations publiques DEVRAIENT veiller :

- à suivre l'approche de **protection de la vie privée dès la conception** et de **sécurité dès la conception** pour sécuriser l'ensemble de leur infrastructure et de leurs modules;
- à ce que les services **ne soient pas vulnérables à des attaques** susceptibles d'interrompre leurs prestations et de causer des vols ou des pertes de données; et
- à respecter les exigences juridiques et les obligations en matière de **protection des données et de la vie privée** en reconnaissant les risques pour la vie privée découlant du traitement et de l'analyse des données avancées.

Elles DEVRAIENT également s'assurer que les contrôleurs se conforment à la législation sur la protection des données en couvrant les points suivants.

- Des « **plans de gestion des risques** » pour identifier les risques, évaluer leur incidence éventuelle et planifier les réponses à apporter au moyen de mesures techniques et organisationnelles appropriées. Compte tenu des évolutions technologiques les plus récentes, ces mesures doivent garantir que le niveau de sécurité est proportionné au degré de risque;
- Des « **plans de continuité des activités** » et des « **plans de sauvegarde et de reprise des activités** » afin qu'il existe des procédures de rétablissement du fonctionnement des opérations après un événement désastreux et afin que toutes les fonctions reviennent à la normale le plus vite possible ;
- Un « **plan d'accès aux données et d'autorisation des données** » qui détermine qui a accès à quelles données et à quelles conditions, pour assurer la protection de la vie privée. Les accès non autorisés et les atteintes à la sécurité devraient faire l'objet d'un suivi et des mesures appropriées devraient être prises pour prévenir toute répétition de ces atteintes ;
- L'utilisation de **services de confiance qualifiés** pour assurer l'intégrité, l'authenticité, la confidentialité et la non-répudiation des données.

Lorsque l'administration publique échange des informations officielles avec d'autres entités, les informations DEVRAIENT être transférées, selon les exigences de sécurité, par le biais d'un réseau sécurisé, harmonisé, géré et contrôlé. Les mécanismes de transfert devraient faciliter des échanges d'informations entre administrations, entreprises et citoyens qui soient :

- **enregistrés et vérifiés**, l'expéditeur et le destinataire sont tous les deux identifiés et authentifiés par le biais de procédures et de mécanismes convenus;
- **chiffrés**, la confidentialité des données échangées est assurée;
- **horodatés**, afin de conserver le moment précis du transfert et de l'accès aux documents électroniques;
- **enregistrés**, des enregistrements électroniques sont conservés afin d'assurer une piste d'audit ayant valeur juridique.

Des mécanismes adéquats DEVRAIENT permettre l'échange sécurisé de messages authentifiés électroniquement, d'enregistrements, de formulaires et d'autres types d'informations entre les différents systèmes; ils DEVRAIENT gérer les exigences de sécurité spécifiques et les services d'identification électronique et de confiance tels que la création et

la vérification de signatures/scellements électroniques ; et ils DEVRAIENT surveiller le trafic pour détecter les intrusions, les changements de données et d'autres types d'attaques. Les informations DOIVENT également être protégées de manière appropriée pendant la transmission, le traitement et le stockage par différents processus de sécurité, tels que :

- la définition et l'application de politiques de sécurité;
- la formation et la sensibilisation à la sécurité;
- la sécurité physique (y compris le contrôle d'accès);
- la sécurité lors du développement;
- la sécurité lors de l'exploitation (y compris le suivi de la sécurité, la gestion des incidents, la gestion des vulnérabilités);
- les examens de sécurité (y compris les audits et les contrôles techniques).

Des exigences communes pour la protection des données DEVRAIENT être convenues avant de fournir des services groupés.

L'échange sécurisé de données nécessite également de recourir à plusieurs fonctions de gestion, parmi lesquelles :

- **la gestion de service,** pour superviser toutes les communications relatives à l'identification, à l'authentification, à l'autorisation, au transfert de données, etc., notamment en ce qui concerne les autorisations d'accès, la révocation d'accès et l'audit;
- **l'inscription auprès du service,** pour fournir un accès, sur autorisation, aux services disponibles par localisation préalable et vérification du caractère fiable du service;
- **la gestion de l'enregistrement des données échangées** pour s'assurer que tous les échanges de données sont consignés, et archivés si nécessaire.

5.13. Les organes de l'administration publique DEVRAIENT prendre en compte les exigences spécifiques en matière de sécurité et de confidentialité et identifier les mesures prévues par l'ANSIE pour la fourniture de chaque service public conformément aux plans de gestion des risques.

5.14. L'administration publique DEVRAIT utiliser les services de confiance prévus par l'ANSIE comme mécanismes garantissant un échange de données sécurisé et protégé dans les services publics.

6 Architecture de l'Interopérabilité

6.1 Concepts Clés

L'architecture de l'Interopérabilité décrit les principes d'architecture et donne une architecture conceptuelle de référence pour le développement des solutions d'e-Gouvernement à Djibouti. Une architecture conceptuelle de référence définit la structure des composants conceptuels, leurs interrelations, ainsi que les principes et directives régissant leur conception et leur évolution dans le temps.

Principe « Une Fois Seulement ». Le modèle proposé garantit le principe selon lequel les informations ne sont fournies aux consommateurs d'informations qu'une seule fois par la source responsable du traitement des informations, et qu'il n'existe aucune autre source d'informations pour la même information. Selon le principe « une fois seulement », les organes publics DEVRAIENT prendre des mesures pour partager des données entre eux, en respectant les règles de confidentialité et de protection des données. Cela nécessite une solution générique et évolutive pour interconnecter différents systèmes. Les données sont conservées uniquement dans une base de données, où elles servent de données de référence. Les exigences de disponibilité PEUVENT conduire à la copie de données, mais dans ce cas, il faut tenir compte du fait que les données PEUVENT être obsolètes.

La société en tant qu'organisation centrée sur les services. Toutes les activités des fonctionnaires, des entreprises, des citoyens, des registres et des systèmes d'information sont considérées comme des services. Les utilisateurs finaux voient les services à travers un portail de services commun. Ils ne s'intéressent pas à l'organisation qui fournit le service, mais au service lui-même. Bien que le secteur privé et le secteur public agissent selon des règles métier assez différentes, les utilisateurs de leurs services sont les mêmes. Par conséquent, il est pratique que les secteurs privés et publics développent et gèrent les services conjointement.

Séparation des systèmes *front-end* et *back-end*. Dans les systèmes d'information du secteur public, les systèmes *front-end* et *back-end* DEVRAIENT être clairement séparés sur le plan architectural. Tous les registres et bases de données du secteur public sont considérés comme des « systèmes *back-end* ». La tâche des systèmes *back-end* est la gestion des données et la fourniture de services réseau ; ils ne traitent pas de l'authentification et de l'autorisation. Par conséquent, il n'est pas nécessaire de créer des composants d'authentification et d'autorisation de l'utilisateur final dans les systèmes *back-end*. Les services web des systèmes *back-end* sont mis à la disposition de l'utilisateur final uniquement par le biais d'intermédiaires de service (systèmes *front-end*).

Réutilisation de composants. Un modèle de service entièrement basé sur des composants pour les organes de l'administration publique permet la mise en place de services publics en réutilisant, autant que possible, les composants de service existants. Les organes de l'administration publique DEVRAIENT convenir d'un schéma commun pour interconnecter les composants faiblement couplés et mettre en place l'infrastructure nécessaire.

Architecture orientée services. Dans l'élaboration de l'architecture informatique de l'État, les principes de l'Architecture Orientée Services (AOS) DOIVENT être suivis. Dans le cas d'une architecture orientée services, différents systèmes fournissent divers services d'information

via les « interfaces de service », qui PEUVENT être utilisées par d'autres systèmes d'information. La description de ces interfaces doit contenir suffisamment d'informations pour l'identification et l'utilisation d'un service, sans que le système utilisateur du service ait besoin de « connaître » quoi que ce soit sur l'architecture interne, la plate-forme, etc. du système fournisseur de services. Dans le cas d'une AOS, l'éditeur du service et le fournisseur de service réel ne doivent pas nécessairement être les mêmes, alors que du point de vue de l'utilisateur du service, cela ne fait aucune différence. Il n'y a aucune restriction quant aux technologies à utiliser pour l'application de l'AOS.

Lier les processus métier via des services groupés. Les systèmes d'information communiquent entre eux via des services groupés. Si, pour l'exécution d'un processus métier dans une structure, des données sont nécessaires ou un flux de travail doit être effectué dans une autre structure, des services groupés sont utilisés. Les structures DEVRAIENT s'assurer que les données et les services qu'elles offrent pourraient être utilisés comme des services groupés. Un service groupé ou un service complexe est combiné à partir de services de base fiables (par exemple, les résultats d'un service de base sont utilisés comme données d'entrée pour un autre). L'utilisateur perçoit un service complexe comme un seul service. Dans le cas des services groupés, une attention particulière doit être portée aux risques liés à la sécurité en rapport avec les droits d'utilisateurs des services ainsi qu'au danger de combiner des données.

Éviter le « point de défaillance unique ». Il est recommandé d'utiliser des solutions où la panne d'une partie du système ne perturbe pas le fonctionnement de l'ensemble du système.

6.1 Les organes de l'administration publique DEVRAIENT construire une solution interopérable en suivant les principes architecturaux convenus.

6.2 Services d'Infrastructures

L'infrastructure de l'Interopérabilité représente un ensemble de systèmes informatiques qui soutiennent la prestation de services publics aux organes administratifs, aux citoyens et aux entreprises. Un composant du système peut être de nature technique (ex : module d'authentification, registre de service) mais aussi de nature fonctionnelle (ex: méthodologie, modèle). Il existe deux types de services : les services métiers et les services d'infrastructure. Un service d'infrastructure est une fonctionnalité technique générique d'un système qui a la charge de fournir un ou plusieurs services métier. Les services d'infrastructure sont masqués pour les utilisateurs finaux.

Nous suivons l'approche **Orientée Service**. Cela signifie que les activités de chaque organisation sont des services. Un service peut être :

- une activité répétitive, un comportement discret qu'un composant de l'organisation effectuerait sous une requête ou un déclencheur.
- un élément de comportement qui fournit des fonctionnalités spécifiques en réponse aux demandes d'acteurs ou d'autres services.

La vue d'ensemble de l'architecture de l'Interopérabilité est illustrée à l'Image 4, elle est structurée selon les modèles architecturaux suivants :

- La vue Juridique ;
- La vue Organisationnelle ;
- La vue Sémantique ;
- La vue Technique (composée d'une partie application et infrastructure) ;
- La vue des principes sous-jacents du CID.

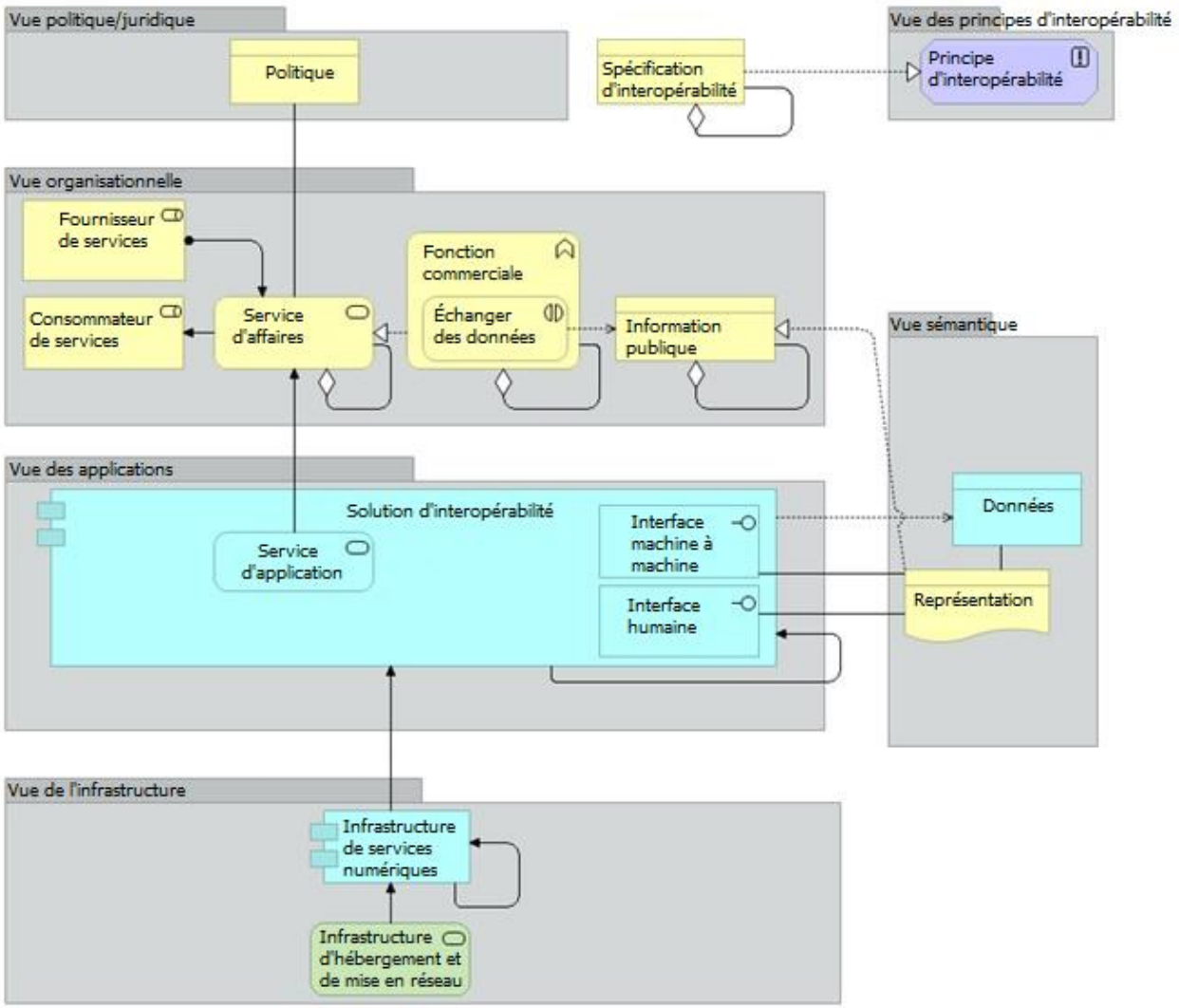

Image 4. Vue d'ensemble de l'architecture de l'Interopérabilité

Afin d'assurer l'interopérabilité des systèmes d'information du secteur public, il développera et mettra en œuvre plusieurs composants communs de l'infrastructure. Les composants catalyseurs les plus importants de l'infrastructure de l'e-gouvernement sont :

- L'écosystème d'échange de données sécurisé
- L'écosystème de l'eID et des services de confiance
- Le catalogue des solutions interopérables
- L'Infrastructure de données ouvertes

- Le point de services uniques

Cette liste de services d'infrastructure n'est pas exhaustive. Les services d'infrastructure tels que le réseau, le *cloud computing*, le paiement, l'infrastructure de données géographiques, le système d'adressage, etc. seront décrits dans des documents séparés.

6.2. Pour parvenir à l'interopérabilité, le gouvernement DEVRAIT développer des services d'infrastructure communs disponibles pour tous les organes de l'administration publique, les entreprises et les citoyens.

6.3. Les services d'infrastructure DEVRAIENT être gratuits pour les organes de l'administration publique, les entreprises et les citoyens.

6.3 L'Écosystème d'Échange de Données Sécurisé

Tous les échanges de données **doivent** se faire de manière sécurisée et contrôlée. La pierre angulaire « échange de données sécurisé » est le facteur le plus crucial pour la mise en œuvre du modèle.

Le concept clé « Séparation des systèmes *front-end* et *back-end* » formulé en 6.1 devrait être pris en charge par l'Écosystème de Données Sécurisé. Les tâches des systèmes *back-end* sont la gestion des données et la délivrance de services en réseau. Les services machine-machine des systèmes *back-end* sont mis à la disposition de l'utilisateur final uniquement par le biais de services intermédiaires (systèmes *front-end*).

Les systèmes *front-end* sont divisés en systèmes internes (par exemple, Intranet) et publics. Les systèmes *front-end* internes sont chargés de gérer les droits d'accès de leurs employés aux services ayant une valeur probante dans le pays. Les droits d'utilisation du service sont personnels et des restrictions peuvent leur être ajoutées (ex : limite de temps d'utilisation d'un service). Les systèmes *front-end* ne devraient pas accorder de droits aux employés d'autres institutions. Les certificats qualifiés sont utilisés pour l'autorisation des services avec valeur probante.

6.4. Les systèmes *back-end* et *front-end* DEVRAIENT être séparés sur le plan architectural.

6.5. Les systèmes *back-end* NE DEVRAIENT PAS être impliqués dans l'authentification et l'autorisation de l'utilisateur final.

6.6. Les services des systèmes *back-end* DEVRAIENT être disponibles pour un utilisateur final uniquement via les systèmes *front-end*.

La sécurité est une préoccupation majeure pour le partage des données et pour la prestation de services publics. Les organes de l'administration publique qui fournissent des services publics devraient garantir :

- à ce que l'ensemble de l'infrastructure et des éléments constitutifs soient sécurisés en respectant les principes d'une approche de confidentialité dès la conception;
- à ce que les services ne soient pas vulnérables aux attaques qui pourraient interrompre leur fonctionnement, provoquer un vol de données ou endommager des données;
- et qu'ils se conforment aux exigences et obligations légales en matière de protection des données et de la vie privée.

Les mécanismes de partage des données devraient faciliter l'échange d'informations entre les organes de l'administration publique, les entreprises et les citoyens qui soient :

- **enregistrés et vérifiés**, l'expéditeur et le destinataire sont tous les deux identifiés et authentifiés par le biais de procédures et de mécanismes convenus;
- **chiffrés**, la confidentialité des données échangées est assurée;
- **horodatés**, afin de conserver le moment précis du transfert et de l'accès aux documents électroniques;
- **enregistrés**, des enregistrements électroniques sont conservés afin d'assurer une piste d'audit ayant valeur juridique.

La vue logique des composants de l'infrastructure de services sécurisés de la Plateforme Nationale d'Interopérabilité et de leurs interconnexions est illustrée dans l'Image 5**.**

L'échange de données sécurisé est basé sur les réseaux TCP/IP. Il existe deux rôles pour les membres des systèmes d'information : les fournisseurs de services (éditeurs, *back end*) et les consommateurs (abonnés, *front end*). Un système d'information peut jouer les deux rôles à la fois : publier ses propres données et en même temps consommer des données publiées par un autre système d'information. Le nombre de membres est illimité. Les composants de la plate-forme sont affichés dans l'Image 5.

Le composant le plus important de la Plateforme Nationale d'Interopérabilité (PNI) est la passerelle. La passerelle encapsule toute la complexité de sécurité pour les membres du système de partage de données. Les passerelles standardisent les processus de transfert de messages entre les membres du système d'échange de données. Seuls l'expéditeur et le destinataire peuvent voir la structure et le contenu des messages.

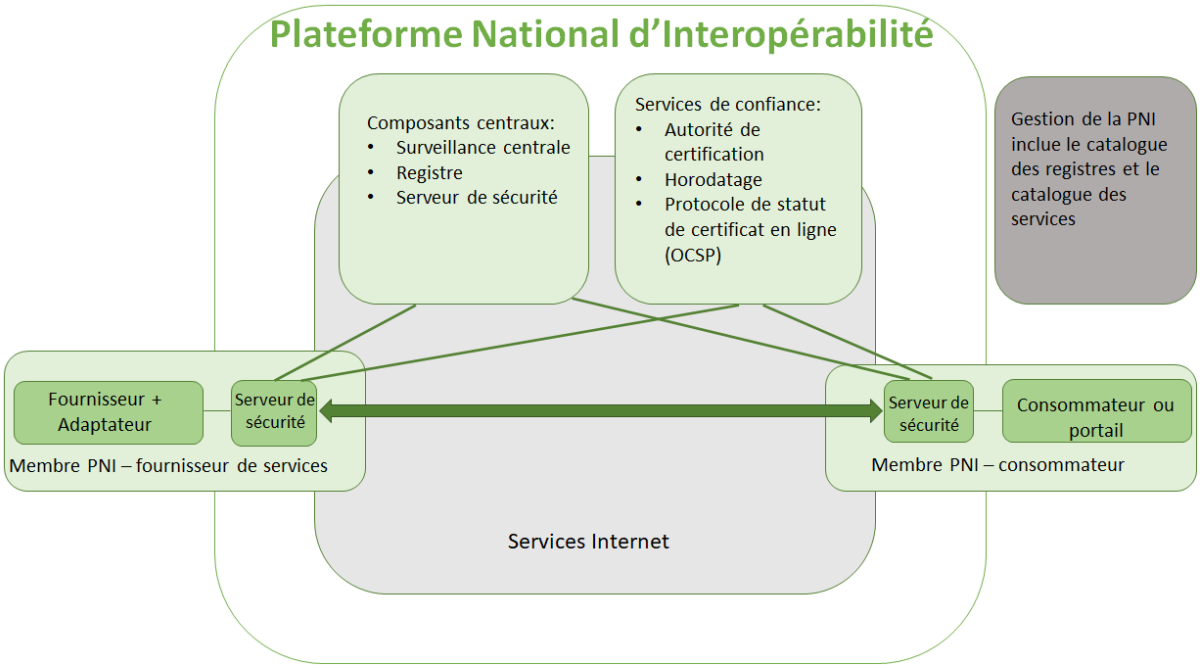

Image 5. Composants de l'infrastructure d'échange de données sécurisé

Le modèle n'implique qu'un nombre minimal de services centraux :

- registre des systèmes d'information et des services,
- identification et authentification par des tierces parties,
- journal des transactions,
- supervision des services,
- et fonctionnalité PKI.

Les composants centraux fournissent des informations aux serveurs proxy sur les participants à l'échange de données. Ces types de mécanismes devraient permettre l'échange sécurisé de messages, d'enregistrements, de formulaires et d'autres types d'informations vérifiés électroniquement entre les différents systèmes. En plus de transporter des données, cette couche doit également gérer des exigences de sécurité spécifiques telles que la création et la vérification de signatures électroniques, le cryptage et l'horodatage. En outre, il devrait y avoir une surveillance du trafic pour détecter les intrusions, les changements de données et d'autres types d'attaques.

La délivrance d'un échange de données sécurisé (c'est-à-dire signé, vérifié, crypté et enregistré) via la plate-forme nationale d'échange de données implique plusieurs fonctions de gestion, notamment :

- Gestion des services pour superviser toutes les communications sur l'identification, l'authentification, l'autorisation, le transport de données, etc., y compris les autorisations d'accès, la révocation et l'audit ;
- Relevé du service pour fournir (sous réserve d'une autorisation appropriée) l'accès aux services disponibles grâce à une localisation préalable et à la vérification de la fiabilité du service ;

- Service d'enregistrement pour veiller à ce que tous les échanges de données sont enregistrés pour preuves futures et archivés en cas de besoin.

Comme ce modèle d'échange de données sécurisé repose sur le principe que les données sont échangées directement entre le fournisseur de données et le consommateur, sans intermédiaire central, il n'a pas de point de défaillance unique. Cela signifie qu'il n'y a pas de point de risque unique pour une cyberattaque ou un dysfonctionnement du système. En cas de défaillance d'un composant, les autres parties peuvent continuer à fonctionner. De plus, les participants peuvent construire leurs systèmes à leur propre rythme sans attendre un développement central.

6.7. L'administration publique DOIT utiliser un écosystème d'échange de données sécurisé pour échanger des données confidentielles.

6.4 Écosystème eID et PKI

L'identité numérique est la pierre angulaire de l'e-gouvernement. En possédant simplement une identification électronique, les citoyens pourront effectuer des transactions électroniques sécurisées et profiter pleinement de l'e-gouvernement en réduisant la lourdeur administrative.

L'**identification électronique** (eID) est le processus d'utilisation des données d'identification d'une personne sous forme électronique, représentant de manière unique soit une personne physique ou morale, soit une personne physique représentant une personne morale.

Le **service de confiance** est un service électronique normalement fourni contre rémunération, qui consiste en :

- la création, la vérification et la validation de signatures électroniques, de cachets électroniques, d'horodatages électroniques, de services d'envoi recommandé électronique et de certificats liés à ces services ; ou alors
- la création, la vérification et la validation des certificats d'authentification de sites Internet ; ou alors
- la conservation des signatures, sceaux ou certificats électroniques liés à ces services.

En construisant l'infrastructure eID et PKI, Djibouti rejoindra les modèles conceptuels de standards internationaux, notamment l'eIDAS[13]. Une vue d'ensemble d'eIDAS est illustrée à l'Image 6.

[13] eIDAS (electronic IDentification, Authentication and trust Services) est un règlement de l'UE sur l'identification électronique et les services de confiance pour les transactions électroniques

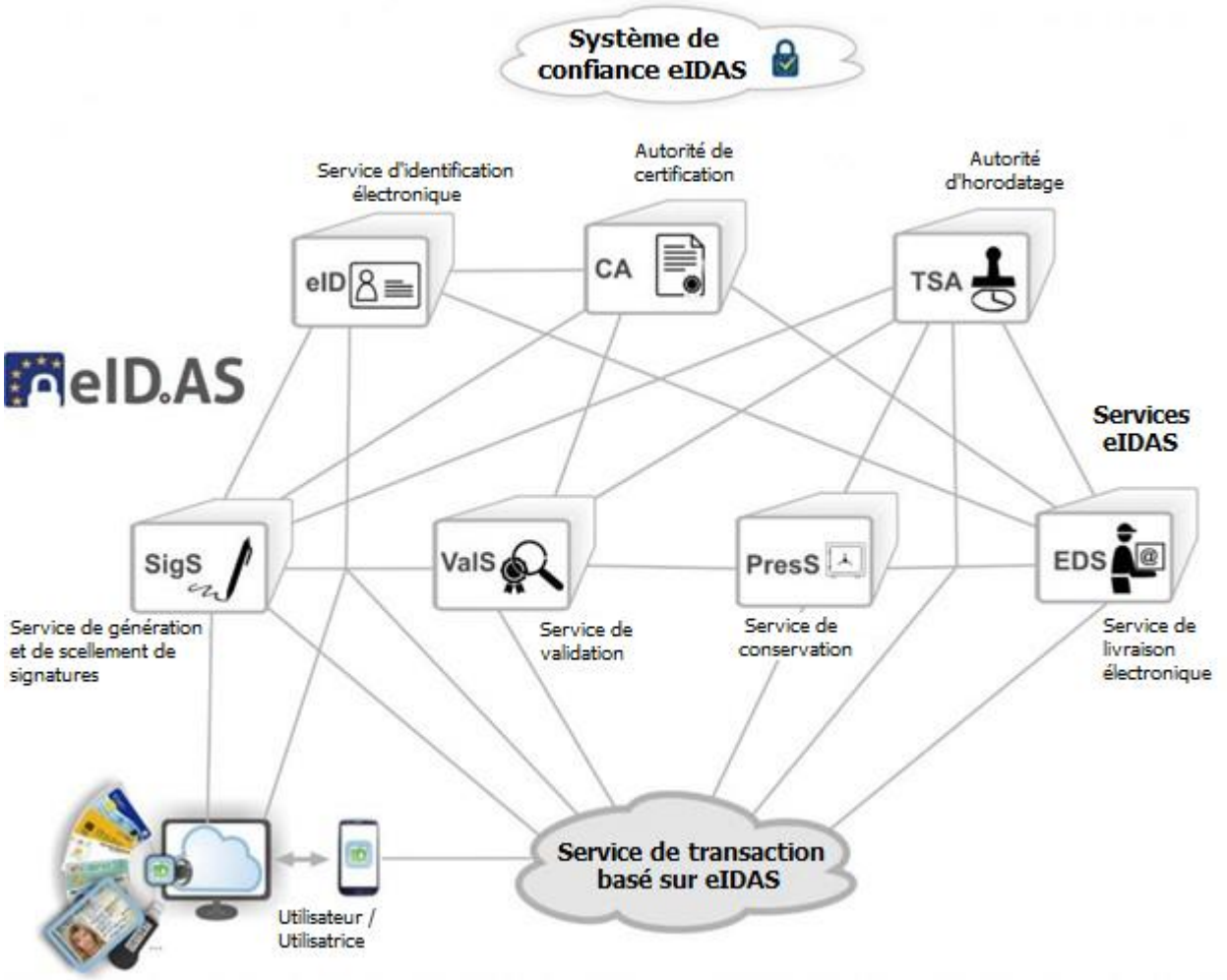

Figure 6. Modèle général d'infrastructure de service eID et de confiance, traduit de https://blog.eid.as/

Service d'identification électronique (eID). Le « Service eID » fournit des services pour l'identification et l'authentification électroniques sécurisées des Utilisateurs et des personnes morales.

Autorité de certification (CA). Une Autorité de Certification (CA) génère des certificats électroniques et les délivre aux Utilisateurs ou à d'autres entités, communément appelées le Sujet d'un certificat.

Autorité d'horodatage (TSA). Prouver l'existence d'un ensemble donné de données numériques à un moment donné est une exigence fondamentale dans de nombreuses transactions électroniques. À cette fin, une autorité d'horodatage (TSA) reçoit les données, qui doivent être horodatées, ou un hachage de celles-ci, et renvoie un jeton d'horodatage, qui est signé par la TSA.

Service de génération et de scellement de signatures (SigS). Le Service de génération et de scellement de signatures (SigS) permet de générer des signatures électroniques (qualifiées).

Service de validation (ValS). Les signatures et sceaux électroniques (qualifiés) générés avec le SigS ci-dessus peuvent être validés auprès du Service de Validation (ValS).

Service de conservation (PresS). La conservation à long terme des documents signés nécessite une forme de conservation qui assure la lisibilité et la validité quel que soit le support de stockage.

Service de livraison électronique (EDS). Le service de livraison électronique ou ESD fait référence à la délivrance de services gouvernementaux via Internet ou d'autres moyens électroniques.

Il est recommandé de construire l'infrastructure eID et PKI de Djibouti en partenariat avec des entités privées (banques, télécoms, autorités de certification, etc.) et des institutions publiques :

- La Direction Générale de la Population et de la Famille (DGPF) est responsable de la gestion des éléments d'identification nominative, personnelle, numérique et biométrique des personnes physiques.
- L'ANSIE est responsable de la gestion de la certification et de la gestion de la délivrance des services de confiance.
- Autres parties prenantes : CNSS, ANEFIP, banques, etc.

6.8. Il est RECOMMANDÉ de construire une infrastructure d'identification électronique et de services de confiance en partenariat avec des entités publiques et privées.

6.5 Le Catalogue des Solutions Interopérables

Les catalogues décrivent des services réutilisables et d'autres actifs pour augmenter leur trouvabilité et leur utilisation. Ce composant permet aux éditeurs de documenter et de mettre à disposition des ressources susceptibles d'être réutilisées par d'autres. Différents types de catalogues existent, par exemple des répertoires de services, des bibliothèques de composants logiciels, des portails de données ouvertes, des registres de registres, des catalogues de métadonnées et des catalogues de normes.

Le catalogue des solutions interopérables (CatIS, Catalogue) est un instrument supplémentaire pour la coordination des systèmes d'information de l'État, un outil de développement et d'administration des systèmes transversaux et un système d'aide à la maintenance des registres de base et des données de référence.

L'objectif du Catalogue est de garantir une gestion transparente, équilibrée et efficace des systèmes d'information du secteur public. Le Catalogue prend en charge l'interopérabilité des bases de données, la gestion du cycle de vie des systèmes d'information et la réutilisation des données, en fournissant des métadonnées complètes et à jour des systèmes d'information du secteur public.

Les composants du catalogue sont :

- **Base de données des institutions**. Fournit des données sur les propriétaires, les administrateurs, les développeurs et les consommateurs de registres et de systèmes d'information. Il comprend des données sur des événements importants : enregistrement des institutions, adhésion des institutions à la PNI, etc.
- **Référentiel de services publics.** Le référentiel décrit les interfaces des utilisateurs des services publics. Ces informations peuvent être utilisées pour créer des portails des usagers de l'administration publique.
- **Registre des registres et systèmes d'information.** Ce composant fournit des métadonnées sur les registres gouvernementaux (DB) et les systèmes d'information (IS) : le nom du DB/IS ; propriétaire ; type de DB/IS ; liste des services ; des informations sur l'enregistrement et l'approbation ; architecture technique ; actes juridiques ; Accords de Niveau de Service ; paramètres de sécurité ; structure logique des données (objets de données, champs de données, paramètres de champs).
- **Référentiel de services de données.** Le référentiel assure l'interopérabilité des systèmes d'information du secteur public et la réutilisation des ressources techniques, organisationnelles et sémantiques. Le référentiel de services est un ajout aux métadonnées conservées dans le registre des registres et comprend les spécifications de tous les services Web et une description détaillée des services gouvernementaux (y compris les descriptions des processus métier).
- **Référentiel d'actifs sémantiques.** Ce référentiel fournit des informations sur les composants réutilisables : actifs sémantiques, directives, etc.

Le Catalogue garantit la transparence de l'administration du système d'information de l'État et aide à planifier la gestion de l'information de l'État. Il fournit des informations sur les sujets suivants :

- Quels systèmes d'information et bases de données sont mis en œuvre dans le secteur public ;
- Quelles données sont collectées et traitées dans quels systèmes d'information ;
- Quels services sont fournis et qui les utilise ;
- Qui sont les sous-traitants responsables et autorisés des systèmes d'information et des bases de données, et qui sont les personnes de contact ;
- Sur quelle base juridique les bases de données sont exploitées et les données traitées;
- Composants réutilisables assurant l'interopérabilité des systèmes d'information (actifs XML, classifications, dictionnaires et ontologies).

Le Catalogue sert d'environnement procédural et administratif pour les actions suivantes :

- Enregistrement et approbation des systèmes d'information et des bases de données ;
- Enregistrement des services ;
- Enregistrement des connexions à la PNI ;
- Administration de composants réutilisables (actifs XML, classifications, dictionnaires et ontologies).

Le Catalogue fournit une assistance digne de confiance et est un excellent outil pour les développeurs, les administrateurs et les utilisateurs du système d'information de l'État. Le Catalogue propose des outils pour coordonner les activités de plusieurs organes de l'administration publique. Les principales parties prenantes du Catalogue sont représentées dans l'Image 7.

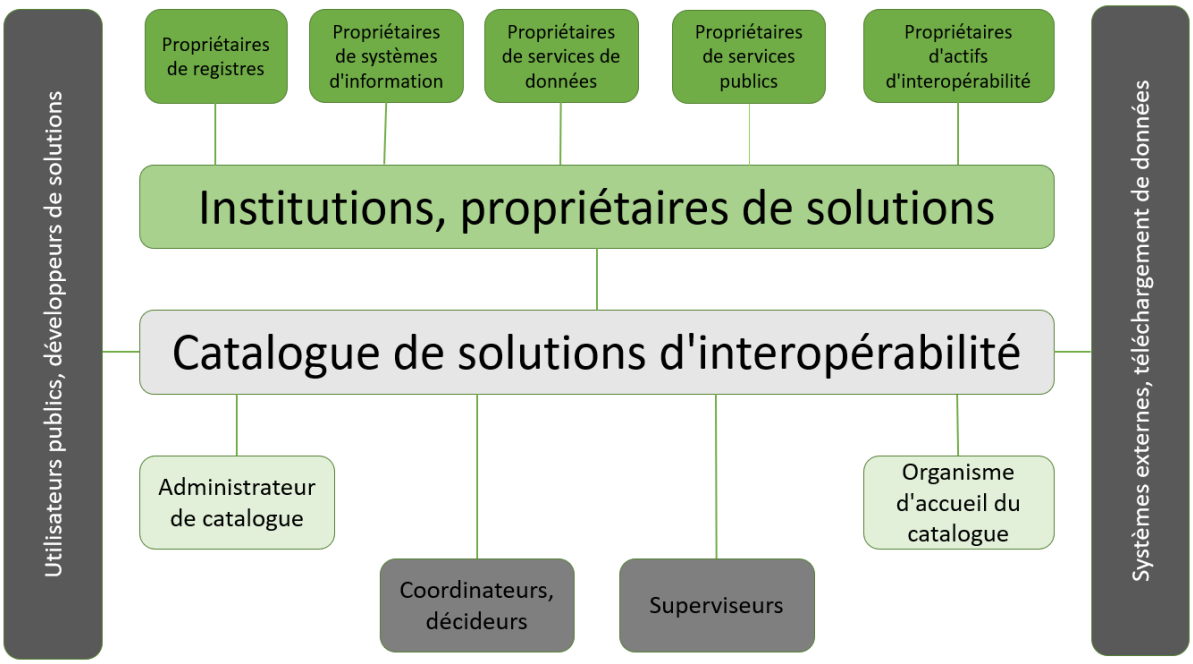

Image 7. Principales parties prenantes de CatIS

Les parties prenantes co-créent le contenu du catalogue. Les experts des institutions soumettent des données sur leurs institutions, les propriétaires de registres fournissent des données sur leurs registres, les propriétaires d'organisations de consommateurs sur leurs systèmes d'information, les propriétaires de services sur leurs services, les propriétaires d'actifs d'interopérabilité sur leurs actifs. Les coordonnateurs et les superviseurs utilisent le catalogue et y enregistreront leurs décisions.

6.9. Les organes de l'administration publique DEVRONT enregistrer leurs systèmes d'information, services et actifs d'interopérabilité dans un catalogue de solutions d'interopérabilité.

6.6 Écosystème de Données Ouvertes

Alors que les gouvernements et les entreprises collectent un large éventail de données, ils ne partagent pas toujours ces données de manière à être facilement découvrables, utilisables ou compréhensibles par le grand public.

Pour permettre une utilisation efficace des données, elles doivent être soumises dans un format lisible par machine ; des règles explicites devraient être établies pour le recyclage des données, garantissant l'interopérabilité des systèmes et services d'information.

L'administration publique DEVRAIT construire un écosystème de données ouvertes pour soutenir le recyclage des données.

La disponibilité des données ouvertes contribuera à :

- **La transparence de la gouvernance** – l'implication des citoyens, leur autonomisation et l'ouverture de la recherche et des biens culturels à leur usage, est une obligation de tous les pays ;
- **L'innovation** – les données ouvertes sont étroitement liées aux initiatives de gouvernement ouvert et aux nouvelles tendances technologiques, telles que les formats ouverts, les logiciels libres, les informations liées, les big data, l'Internet du futur et la co-création ;
- **Stimuler l'économie** – l'ouverture des informations du secteur public permettra aux organisations du secteur privé et du secteur associatif de les combiner avec diverses données et de créer de nouveaux services à valeur ajoutée. Il n'est pas facile d'évaluer l'impact financier possible du recyclage des données sur la société puisqu'il est largement indirect.

L'administration publique a besoin de solutions aux problèmes suivants :

- Développement et mise en œuvre d'une politique de données ouvertes ;
- Accroître la transparence du secteur public, passage du principe « public par défaut » au principe « données ouvertes par défaut » ;
- Utiliser de nouvelles connaissances, innovations et services, créés sur le principe de données ouvertes, pour dynamiser l'économie ;
- Accélérer la transition vers les technologies du futur (technologies de données liées, Internet des Objets, big data et co-création ;

Cela devrait aller de pair avec le développement d'un portail de données ouvertes pour Djibouti.

6.10. Les organes de l'administration publique DEVRONT enregistrer leurs données ouvertes lisibles par machine dans un portail de données ouvertes.

6.7 Point de contact unique

Un portail centralisé des services publics permet aux utilisateurs d'accéder à plusieurs systèmes d'information et portails sans avoir besoin de se connecter plusieurs fois. Il permet l'accès à un certain nombre de e-services. L'accès au système est possible avec ou sans eID et, selon la méthode d'accès, le nombre de service disponible varie. Le portail centralisé est le portail web officiel du gouvernement, il est déployé et maintenu par l'ANSIE.

Le portail centralisé comportera des thématiques à destination de trois principaux acteurs à savoir : les citoyens, les entreprises, les acteurs de l'administration publique et les visiteurs. Il est recommandé que le portail centralisé élabore un environnement personnel sécurisé pour les citoyens, accessibles par eID ou mobileID. La rubrique personnelle peut inclure les éléments suivants :

- **Zone Cycle de vie.** Il contient des articles sur la façon de résoudre des problèmes importants ou fréquents (comme une demande de prestations familiales) et des conseils sur ce qu'il faut faire dans certaines situations. Les services en ligne, les articles et les coordonnées du portail sont liés pour permettre aux personnes de trouver facilement des informations relatives à certains sujets.
- **Espace e-service** permet aux gens de vérifier les données que le gouvernement a recueillies à leur sujet ;
- **Services de Notification** par exemple interruptions dans les livraisons d'électricité ou d'eau, expiration d'une période de validité, etc.) ;
- **Espace Demandes** permet aux personnes de remplir des formulaires puis de les transmettre aux institutions concernées ;
- **Espace de Documents Sécurisés** permet aux utilisateurs de signer des documents et de les transmettre.

Le sous-système du portail permet aux utilisateurs finaux d'accéder aux services électroniques de manière unifiée décrite ci-dessous.

- **Portail citoyen** – services pour le grand public. L'utilisation du portail est pratique et sécurisée et permet de gagner du temps. Les citoyens et les étrangers peuvent trouver sur le portail des informations sur leurs droits et obligations dans la communication avec les autorités publiques djiboutiennes. Les informations détaillées que contient le portail peuvent être utilisées pour trouver des réponses à des questions potentiellement délicates avant qu'elles ne surviennent. Les requêtes envoyées via le portail sont traitées directement par le support utilisateur ou transmises au service concerné – les utilisateurs n'ont pas besoin de le faire eux-mêmes. Toutes les questions peuvent être soumises en un seul endroit, avec une réponse garantie. Chacun peut accéder à ses données. De plus, les citoyens peuvent voir qui a consulté leurs données personnelles dans les registres. Cela permet d'éviter une utilisation abusive des données personnelles.
- **Portail des officiels** – services aux fonctionnaires. Le portail est un environnement sécurisé via lequel les utilisateurs disposent d'un accès pratique aux informations, services et coordonnées du secteur public. Les fonctionnaires obtiennent le soutien du portail pour ouvrir leurs propres ressources via le portail centralisé.
- **Portail des entreprises** – services pour les utilisateurs des entreprises. Le portail est un moyen simple et sécurisé d'obtenir des informations sur le lancement et la gestion d'une entreprise et sur la communication avec les services publics. Si l'exploitation dans un certain domaine est soumise à des exigences spécifiques, le portail fournit aux entreprises les démarches à suivre. Pour les opérateurs économiques, le portail représente un point de contact unique.

6.11. Un point de contact unique DEVRAIT être mis à la disposition des utilisateurs, pour masquer la complexité administrative interne et faciliter l'accès aux services publics, par ex. lorsque plusieurs organes doivent travailler ensemble pour fournir un service public.

7 Conclusion

Au cours des dernières décennies, les organes de l'administration publique de Djibouti ont investi dans les TIC pour moderniser leurs opérations internes, réduire les coûts et améliorer les services qu'ils offrent aux citoyens et aux entreprises. Malgré les progrès significatifs réalisés et les bénéfices déjà obtenus, ils restent confrontés à des obstacles considérables à l'échange d'informations et à la collaboration électronique. Il s'agit notamment des barrières juridiques ; des processus métier et des modèles d'information incompatibles ; et de la diversité des technologies utilisées. En effet, historiquement, les systèmes d'information ont été mis en place dans le secteur public indépendamment les uns des autres et non de manière coordonnée.

Le CID promeut la communication électronique entre les organes de l'administration publique en fournissant un ensemble de modèles, de principes et de recommandations communs. Il reconnaît et souligne le fait que l'interopérabilité n'est pas seulement une question de TIC, car elle a des niveaux d'implications allant du juridique aux techniques. Le CID identifie quatre niveaux de défis d'interopérabilité (juridique, organisationnelle, sémantique et technique) tout en soulignant le rôle essentiel de la gouvernance pour assurer la coordination des activités pertinentes à tous les niveaux et secteurs de l'administration.

Le modèle conceptuel des services publics couvre la conception, la planification, le développement, l'exploitation et la maintenance de services publics intégrés à tous les niveaux gouvernementaux, du niveau local au niveau central du gouvernement. Les principes énoncés ici guident la prise de décision sur la mise en place de services publics interopérables. Par ailleurs, le CID propose des outils pratiques sous la forme d'un ensemble de recommandations pour action. L'unité centrale de coordination ANSIE DOIT avoir un mandat clair de la Présidence. Il est important que l'unité centrale de coordination rende compte directement à la Présidence, pour s'assurer que les décisions et les progrès auront un soutien politique de haut niveau et des ressources disponibles.

Afin d'assurer l'interopérabilité des systèmes d'information du secteur public, le secteur public développera et mettra en œuvre plusieurs composants d'infrastructure communs. Les composants/catalyseurs les plus importants de l'infrastructure de l'e-Gouvernement djiboutien sont :

- L'écosystème d'échange de données sécurisé
- L'eID et l'écosystème des services de confiance
- Le catalogue des solutions interopérables
- L'infrastructure de données ouvertes
- Un point de contact unique

Le cadre énonce des principes et donne des recommandations concrètes pour la construction de ces services d'infrastructure.