XROAD BJ

Cadre d'interopérabilité

institué par le décret
n° 2020-209
du 18 mars 2020

Le cadre d'interopérabilité du Bénin

institué par le décret
n° 2020-209 du 18 mars 2020

MINISTÈRE DU NUMÉRIQUE ET DE LA DIGITALISATION
RÉPUBLIQUE DU BÉNIN

ASSI AGENCE DES SERVICES ET SYSTÈMES D'INFORMATION
PRÉSIDENCE DE LA RÉPUBLIQUE DU BÉNIN

XROAD BJ

Table des matières

Table des figures

XROAD BJ

Le cadre d'interopérabilité

1 ◆ INTRODUCTION

1.1. Définition

L'interopérabilité désigne, au sens du présent cadre, l'aptitude d'organisations disparates et diverses à interagir en vue de la réalisation d'objectifs communs mutuellement avantageux, décidés et arrêtés d'un commun accord, impliquant le partage d'informations et de connaissances entre ces organisations à travers les processus métiers qu'elles prennent en charge, grâce à l'échange de données entre leurs systèmes d'information respectifs.

Elle est à la fois une condition préalable et un facilitateur de la prestation efficace des services publics dans le cadre de la dématérialisation de l'administration béninoise. C'est la capacité de faire en sorte que les systèmes et les organisations fonctionnent ensemble (inter-opèrent). Dans le présent document, le terme « interopérabilité » est utilisé de manière large. Il prend en compte non seulement des facteurs techniques mais également des facteurs sociaux, politiques et organisationnels.

1.2. Objectifs du Cadre d'Interopérabilité

Le cadre d'interopérabilité (CdI) est destiné à améliorer la coopération entre structures de l'administration publique en vue de la mise en place de services publics via un portail unique. À ce titre il permet :

- **l'échange des informations entre structures de l'administration publique** pour satisfaire aux exigences légales ou aux engagements politiques ;
- **le partage et la réutilisation des informations auprès des structures de l'administration publique** pour accroître l'efficacité administrative et réduire la charge administrative pesant sur les citoyens et les entreprises ;
- **la réduction des coûts pour les structures de l'administration publique, les entreprises et les citoyens** grâce à une prestation efficace des services publics.

Le CdI est un ensemble d'accords et de lignes directrices visant à garantir la fourniture de services aux structures de l'administration publique, aux entreprises et aux citoyens. Le cadre d'interopérabilité béninois sert comme :

- **un guide pour l'élaboration de concepts** pour les systèmes d'information à l'échelle nationale (facilitateurs d'interopérabilité) ;
- **un guide destiné aux responsables de projets informatiques** de l'administration publique pour l'élaboration de concepts pour les systèmes d'information de leurs institutions ;
- **une référence aux exigences nécessaire à la fourniture de certains services publics.**

Les objectifs spécifiques du cadre d'interopérabilité béninois sont les suivants :

- **faciliter la transformation de l'administration publique** en une administration centrée sur les services, dans laquelle tous les citoyens peuvent communiquer avec l'État indépendamment de la structure hiérarchique et de la division des rôles des institutions gouvernementales ;
- **réduire les charges liées à la dématérialisation du secteur public** grâce à une large utilisation de règles et de solutions communes ;
- **améliorer l'interopérabilité des nouveaux projets numériques** grâce à l'utilisation coordonnée de services d'infrastructure communs développés de manière centralisée et suivant des normes ouvertes;
- **améliorer la coordination et la gestion des systèmes d'information de l'État** et accélérer le développement de contenus numériques adaptés ;
- **contribuer au développement harmonieux du système d'information de l'État ;**
- **permettre le développement autonome de tous les systèmes d'information** dans le respect des principes d'interopérabilité organisationnelle, sémantique et technique.

1.3. Avantages

Les principaux avantages liés à la mise en œuvre du cadre d'interopérabilité sont notamment :

- **contribuer à l'ouverture des systèmes d'information des Administrations** et promouvoir l'échange d'informations entre Administrations ;
- **améliorer la qualité des services fournis aux usagers** par la mise en cohérence des services dématérialisés proposés aux usagers et des échanges d'informations accrus entre les ministères et autres institu-

tions de l'État ;

- **pérenniser les systèmes d'information publics** par l'emploi de normes et standards reconnus internationalement ;
- **maîtriser et réduire les coûts de développement, de maintenance et les délais** de mise en œuvre des services de l'Administration Électronique ;
- **faciliter la diffusion de bonnes pratiques de développement des systèmes d'information.**

1.4. Élaboration et mise à jour du CdI

1.4.1. Élaboration

La présente version du cadre d'interopérabilité a été élaborée sur la base d'un état des lieux de l'existant et de benchmarks internationaux quant aux principes de base, modèles et recommandations d'interopérabilité. Elle s'applique à toute réalisation de projets numériques dans l'administration béninoise.

Elle prend en compte les commentaires des acteurs béninois publics et privés des TIC.

Elle est la toute première au Bénin et les parties prenantes sont tenues de suivre les recommandations qui y sont contenues.

1.4.2. Mise à jour

Le cadre d'interopérabilité doit fréquemment être mis à jour et adapté aux évolutions technologiques et aux besoins d'interopérabilité pour une administration électronique.

2 ◆ PRÉSENTATION DU CADRE D'INTEROPÉRABILITÉ

2.1. Périmètre du cadre d'interopérabilité

Le champ d'application du CdI couvre trois types d'interactions :

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

Ainsi, différents types d'acteurs prennent part aux échanges couverts par le périmètre du CdI :

- **le terme « Usager »** recouvre les notions suivantes :
  - usager « Citoyen », personne physique ;
  - usager « Entreprise », personne morale.
- **l'« Agent Public »,** personne physique agissant au nom d'une Administration ;
- **le Système d'Information d'une entreprise,** entité technique ;
- **le Système d'Information d'une administration,** entité technique.

2.2. Présentation des niveaux d'interopérabilité

Différents niveaux d'interopérabilité sont à prendre en compte pour assurer un échange réussi entre les parties prenantes.

La présente version du CdI en identifie cinq (05) :

2.2.1. Niveau politique

L'établissement d'un nouveau service public béninois est le résultat d'une action directe ou indirecte au niveau politique. Si cet établissement

résulte d'un nouvel instrument législatif, le champ d'application, les priorités et les ressources nécessaires à l'établissement et à l'exploitation du service doivent être définis au moment même où le nouvel instrument législatif est adopté. Cependant, un soutien politique est également nécessaire dans les cas où les nouveaux services ne sont pas directement liés à un nouvel instrument législatif mais sont créés dans le but de fournir des services publics mieux centrés sur l'utilisateur et de meilleure qualité.

De même, un soutien politique est nécessaire aux efforts d'interopérabilité mis en œuvre dans le but de faciliter la coopération entre administrations publiques. Pour qu'une telle coopération soit efficace, les parties prenantes doivent partager la même vision, s'accorder sur des objectifs communs et harmoniser leurs priorités. Une action au niveau intersectoriel ne peut être fructueuse que si toutes les parties prenantes accordent une priorité et des ressources suffisantes à leurs efforts respectifs d'interopérabilité mis en œuvre dans le but d'atteindre des objectifs communs dans les délais convenus.

2.2.2. Niveau juridique

Chaque administration publique contribuant à la fourniture d'un service public travaille dans son propre cadre juridique. L'interopérabilité juridique consiste à garantir que les organisations fonctionnant sous différents cadres juridiques, politiques et stratégiques puissent fonctionner ensemble. Cela pourrait exiger que la législation ne bloque pas la mise en place de services publics électroniques et qu'il existe des accords clairs sur la manière de traiter les différences de législation, y compris la possibilité de mettre en place une nouvelle législation.

RECOMMANDATION 1

Le Bénin doit s'assurer que la législation est filtrée au moyen de « contrôles d'interopérabilité » afin d'identifier tout obstacle à l'interopérabilité. Lors de la rédaction d'une législation visant à créer un service public, il faudra essayer de la rendre conforme à la législation en vigueur, effectuer un « contrôle numérique » et prendre en compte les exigences de protection des données.

Une étape vers l'interopérabilité juridique consiste à effectuer des « contrôles d'interopérabilité » en examinant la législation existante afin de recenser les éventuels obstacles à l'interopérabilité tels que les restrictions sectorielles ou géographiques dans l'utilisation et le stockage des données, des modèles de licence de données différents et vagues, des exigences trop strictes imposant d'utiliser des technologies numériques spécifiques ou des modes de prestation de services particuliers, des besoins obsolètes en matière de sécurité et de protection des données, etc.

Ensuite, considérant que les services publics béninois sont clairement destinés à être fournis entre autres et notamment par voie électronique, les TIC doivent être pris en compte le plus tôt possible dans le processus législatif.

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

2.2.3. Niveau organisationnel

L'interopérabilité organisationnel est relative à la manière dont les organismes du secteur public alignent leurs processus métier, leurs responsabilités et leurs attentes pour atteindre des objectifs convenus d'un commun accord et mutuellement bénéfiques. Dans la pratique, l'interopérabilité organisationnelle consiste à documenter et à intégrer ou à 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. Pour permettre à différents organismes du secteur public de collaborer efficacement en vue de fournir de meilleurs services, il peut être nécessaire de procéder à une harmonisation de leurs processus métier existants, voire de définir et de mettre en place 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 organismes contribuant à la prestation de services puissent comprendre le processus métier global et le rôle qu'elles y jouent.

Afin d'assurer une interopérabilité organisationnelle optimale, les relations organisationnelles et notamment celles entre les prestataires de services et leurs utilisateurs doivent être clairement établies. Il faut trouver pour cela les instruments nécessaires à la formalisation de l'assistance mutuelle, de l'action conjointe et des processus métier interconnectés dans le contexte de la prestation d'un service.

RECOMMANDATION 2

Documenter les processus commerciaux à l'aide de techniques de modélisation communément acceptées et s'accorder sur la manière dont ces processus doivent être alignés pour fournir un service public béninois.

RECOMMANDATION 3

Publier les processus dans le catalogue des actifs d'interopérabilité.

RECOMMANDATION 4

Clarifier et formaliser les relations organisationnelles pour l'établissement et le fonctionnement de services publics.

2.2.4. Niveau 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 cadre du présent document, 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 communicantes ;
- **l'aspect syntaxique consiste à définir le format exact (structure et type de fichier) du fichier,** qui devra être lisible par une machine, qui sera utilisé pour échanger les données.

Un point de départ pour améliorer l'interopérabilité sémantique est de considérer les données et les informations comme un bien public d'une grande valeur. Une stratégie de gestion de l'information devra être élaborée et coordonnée au niveau le plus élevé possible pour éviter la fragmentation et fixer des priorités. Par exemple des 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.

RECOMMANDATION 5

Considérer les données et informations comme un actif public devant être générées, collectées, gérées, partagées, protégées et préservées de manière appropriée.

RECOMMANDATION 6

Mettre en place, au plus haut niveau possible, une stratégie de gestion de l'information pour éviter la fragmentation et la duplication. La gestion des métadonnées, des données de base et des données de référence doit être priorisée.

Des approches telles que la conception fondée sur les données (data-driven-design), associées à des technologies de données liées, sont des moyens permettant d'améliorer sensiblement l'interopérabilité sémantique.

Aussi bien que les normes techniques favorisent l'interopérabilité technique (par exemple la connectivité réseau), des normes et spécifications d'information solides, cohérentes et universellement applicables sont nécessaires pour permettre un échange d'informations utile entre les organismes du secteur public.

2.2.5. Niveau technique

L'interopérabilité technique couvre les applications et les infrastructures reliant entre eux 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 souvent un obstacle majeur à l'interopérabilité. Il s'agit malheureusement souvent, vu leur développement fréquent dans des contextes historiques très différents et pour les besoins d'un domaine bien spécifique et isolé, d'îlots TIC fragmentés pour lesquels il est difficile d'assurer une interopérabilité standardisée et optimale. Il n'est cependant pas possible de remplacer tous les services d'un coup. Cela n'est pas non plus toujours nécessaire et urgent pour tous les services, vu que certains services ne sont guère utilisés de manière transversale et présentent donc moins de besoins en interopérabilité. Il faut cependant définir un plan qui identifie les systèmes vieillissants qui ont une importance majeure pour les organismes du secteur public en matière d'interopérabilité (des échanges de données fréquents, des services qui ont vocation à réutilisation fréquente, des services clés, etc.) et viser à remplacer prioritairement et rapidement les plus importants.

L'interopérabilité technique doit être assurée, si possible, par l'utilisation de spécifications techniques formalisées. Ces spécifications doivent, dans la mesure du possible, être des spécifications ouvertes.

RECOMMANDATION 7

Utiliser des spécifications ouvertes, le cas échéant, pour assurer l'interopérabilité technique lors de l'établissement de services publics.

2.3. Principes généraux d'interopérabilité

Les principes énoncés ci-dessous sont des principes généraux d'interopérabilité pertinents pour la mise en place de systèmes et de services d'information béninois. S'appliquant au processus de création de services publics, Ils ont été inspirés du cadre d'interopérabilité européen et adaptés à l'environnement béninois. Au nombre de douze, ils sont regroupés en quatre catégories conformément aux informations ci-après.

2.3.1. Principe fixant le contexte des actions

◆ SUBSIDIARITÉ ET PROPORTIONNALITÉ

Subsidiarité : Le principe de subsidiarité suppose que les décisions de la politique informatique béninoise sont prises aussi près que possible des institutions publiques, des entrepreneurs et des citoyens. En d'autres

termes, le l'État ne prend des mesures que si celles-ci sont plus efficaces que les mesures prises au niveau local. L'application du principe de subsidiarité signifie que les solutions centralisées sont utilisées le moins possible.

Proportionnalité : Au niveau central, seuls les services d'infrastructure communs (infrastructure à clé publique, système d'échange de données sécurisé, catalogue des systèmes d'information de l'État) et les systèmes fournissant des services communs aux citoyens à partir d'institutions du secteur public (par exemple un portail pour les citoyens) sont utiles. Les ministères n'imposent pas de solutions centralisées dans leurs secteurs de gouvernement, où une institution peut perdre le contrôle des processus opérationnels. Le gouvernement central ne prescrit pas non plus de solutions techniques aux gouvernements locaux. Dans le même temps, le principe de proportionnalité ne limite pas la coopération des institutions du secteur public dans la recherche de solutions standard communes.

Les systèmes d'information supportent les structures organisationnelles existantes et leurs objectifs. C'est pourquoi la fusion mécanique des systèmes d'information de différentes organisations doit être évitée, si possible. Au lieu de cela, la création de systèmes d'information indépendants, liés par des services est privilégiée.

RECOMMANDATION 8
Les institutions béninoises du secteur public doivent aligner leurs cadres et leurs stratégies sur ceux du CdI.

RECOMMANDATION 9
Les décisions politiques relatives aux technologies de l'information béninoises ne sont exécutées que si elles sont plus efficaces que celles prises dans les institutions du secteur public.

RECOMMANDATION 10
Au lieu de centraliser les systèmes d'information, ils doivent être mutuellement liés par des services.

2.3.2. Principes d'interopérabilité fondamentaux

◆ OUVERTURE

Le concept d'ouverture concerne principalement les données, les spécifications et les logiciels. Les données gouvernementales ouvertes renvoient à l'idée que toutes les données publiques doivent être librement disponibles pour être utilisées et réutilisées par des tiers, sauf si des restrictions s'appliquent, par exemple pour la protection des données personnelles, la confidentialité ou les droits de propriété intellectuelle.

Un organe administratif béninois doit être tenu de veiller à ce que les informations publiques soient publiées de manière proactive sur ses propres ressources électroniques (appropriées). Les informations publiques publiées de manière proactive doivent être ouvertes et également disponibles pour toute personne. Il est inadmissible de facturer des frais ou d'introduire toute autre restriction d'accès aux informations publiques publiées de manière proactive, sauf dans les cas prévus par la loi.

L'utilisation de technologies et de produits logiciels open source peut permettre de réduire les coûts de développement, d'éviter un effet de blocage et de permettre une adaptation rapide à des besoins métier spécifiques, car les communautés de développeurs qui les prennent en charge les adaptent en permanence. Les administrations publiques doivent non seulement utiliser des logiciels open source, mais aussi chaque fois que possible, contribuez aux communautés de développeurs pertinentes. L'open source est un catalyseur du principe sous-jacent de la réutilisabilité.

Le niveau d'ouverture d'une spécification (ou norme) est déterminant pour la réutilisation de composants logiciels mettant en œuvre cette spécification. Si le principe de transparence s'applique pleinement :

- **toutes les parties prenantes ont la possibilité de contribuer à l'élaboration de la spécification** et un examen public fait partie du processus de prise de décision ;
- **la spécification est disponible** pour être étudiée par tout le monde ;
- **les droits de propriété intellectuelle sur le cahier des charges sont concédés sous les termes de la licence FRAND**[1], d'une manière qui permet une implémentation à la fois dans les logiciels propriétaires et dans les logiciels open source[2], et de préférence sans redevance.

L'effet positif des spécifications ouvertes est démontré par l'écosystème Internet. Cependant, les administrations publiques peuvent décider d'utiliser des spécifications moins ouvertes si celles qui existent ne répondent pas aux besoins fonctionnels. Dans tous les cas, les spécifications doivent être mûres et suffisamment prises en charge par le marché, sauf si elles sont utilisées pour créer des solutions innovantes.

RECOMMANDATION 11
Les administrations doivent publier les données qu'elles possèdent sous forme de données ouvertes, à moins que certaines restrictions ne s'appliquent.

RECOMMANDATION 12
Assurer des règles de jeu équitables aux logiciels à code source ouvert et démontrer une considération active et équitable de l'utilisation d'un logiciel à code source ouvert, en tenant compte du coût total de possession de la solution.

RECOMMANDATION 13
Les administrations 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.

◆ TRANSPARENCE

La transparence dans le contexte du CdI consiste à :

- **activer de la visibilité dans l'environnement administratif d'une administration publique.** Il s'agit de permettre à d'autres administra-

tions publiques, citoyens et entreprises de visualiser et de comprendre les règles administratives, les processus, les données, les services et la prise de décision.

› **assurer la disponibilité des interfaces avec les systèmes d'information internes.** Les administrations publiques exploitent un grand nombre de systèmes d'information souvent hétérogènes et disparates à l'appui de leurs processus internes. L'interopérabilité dépend de la disponibilité d'interfaces avec ces systèmes et des données qu'ils traitent. L'interopérabilité facilite à son tour la réutilisation des systèmes et des données et permet leur intégration dans des systèmes plus vastes.

RECOMMANDATION 14
Les administrations sont tenues d'assurer la visibilité interne et de fournir des interfaces externes pour les services publics béninois.

› **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, détenus et gérés par les administrations publiques.

◆ RÉUTILISABILITÉ

La réutilisation signifie que les 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 pour le problème en question et, le cas échéant, en adoptant des solutions qui ont fait leurs preuves ailleurs. Cela nécessite que l'administration publique soit disposée à partager ses solutions, concepts, cadres, spécifications, outils et composants d'interopérabilité avec d'autres.

RECOMMANDATION 15
Les administrations publiques béninoises doivent réutiliser et partager des solutions et coopérer à l'élaboration de solutions communes.

RECOMMANDATION 16
Les administrations béninoises doivent réutiliser et partager des informations et des données, à moins que certaines restrictions de confidentialité ou de vie privée ne s'appliquent.

La réutilisation des solutions informatiques (composants logiciels, interfaces de programmation d'applications, normes, par exemple), des informations et des données facilite l'interopérabilité et améliore la qualité, car elle prolonge l'utilisation opérationnelle, tout en permettant des économies de temps et d'argent. Ces normes et spécifications existantes peuvent et devraient être utilisées plus largement au-delà du domaine pour lequel elles ont été initialement développées.

◆ NEUTRALITÉ TECHNOLOGIQUE ET PORTABILITÉ DES DONNÉES

Lorsqu'elles établissent des systèmes et des services d'information, les administrations publiques doivent se concentrer sur les besoins fonctionnels et différer le plus 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 l'environnement technologique en rapide évolution. Les administrations publiques doivent rendre l'accès aux services publics indépendant de toute technologie ou produit spécifique.

Le principe exige que les données puissent être facilement transférées entre différents systèmes pour éviter le blocage, favoriser la libre circulation des données et assurer des conditions de concurrence équitables. La portabilité des données est la capacité de déplacer et de réutiliser facilement des données entre différents systèmes et applications.

RECOMMANDATION 17
Les administrations publiques béninoises ne doivent pas imposer de solutions technologiques spécifiques disproportionnées aux citoyens, aux entreprises et aux autres administrations lors de l'établissement de systèmes et de services d'information.

RECOMMANDATION 18
Lors du développement de la fonctionnalité des systèmes d'information, les décisions technologiques doivent être prises le plus tard possible.

RECOMMANDATION 19
Les administrations publiques doivent s'assurer que les données sont facilement transférables entre systèmes et applications.

RECOMMANDATION 20
Les interfaces des systèmes d'information doivent être créées de manière neutre sur le plan technologique, en utilisant des normes ouvertes, prescrites dans le cadre d'interopérabilité (XML, WSDL, SOAP, REST, etc.).

2.3.3. Principes relatifs aux besoins et attentes génériques des utilisateurs

◆ CENTRÉ SUR L'UTILISATEUR

Les utilisateurs des services publics béninois sont censés être toute administration publique, citoyen ou entreprise, accédant à ces services et en bénéficiant. Les besoins des utilisateurs doivent être pris en compte pour déterminer quels services publics devraient être fournis et comment ils devraient être fournis.

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

› **une approche de fourniture de service multicanal,** signifiant la disponibilité de canaux alternatifs, physiques et numériques, pour accéder à un service, constitue un élément important de la conception du

service public, les utilisateurs pouvant préférer des canaux différents en fonction des circonstances et de leurs besoins.

- **un point de contact unique doit être mis à la disposition des utilisateurs,** afin de masquer la complexité administrative interne et de faciliter l'accès aux services publics, par exemple lorsque plusieurs organismes doivent collaborer pour fournir un service public.
- **les commentaires des utilisateurs doivent être systématiquement recueillis,** évalués et utilisés pour concevoir de nouveaux services publics et améliorer encore ceux existants.
- dans la mesure du possible, en vertu de la législation en vigueur, **les utilisateurs devraient pouvoir fournir des données une seule fois** et les administrations doivent être en mesure de récupérer et de partager ces données pour servir l'utilisateur, conformément aux règles de protection des données.
- **les utilisateurs doivent être invités à ne fournir que les informations absolument nécessaires** pour obtenir un service public donné.

RECOMMANDATION 21
L'utilisateur doit être en mesure de choisir un type de canal de service acceptable : bureau de service, poste, téléphone, courrier électronique et autres canaux Internet.

RECOMMANDATION 22
Une personne identifiée par un identifiant électronique ou par un autre moyen sécurisé doit être en mesure de demander tout service public électronique.

RECOMMANDATION 23
Le portail citoyen doit agir comme un point de contact unique pour les services publics. Il est recommandé que plusieurs administrations travaillent ensemble pour fournir des services agrégés via un portail citoyen.

RECOMMANDATION 24
Les commentaires des utilisateurs doivent être systématiquement recueillis, évalués et utilisés comme base pour l'amélioration future des services. Mettre en place des mécanismes pour impliquer les utilisateurs dans l'analyse, la conception, l'évaluation et le développement ultérieur des services publics béninois.

RECOMMANDATION 25
Les données doivent être fournies par les utilisateurs une seule fois, et les administrations doivent 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.

RECOMMANDATION 26
L'approche institutionnelle doit être remplacée par une approche utilisateur. Les institutions doivent fournir des informations de leur propre initiative.

◆ INCLUSION ET ACCESSIBILITÉ

L'inclusion consiste à **permettre à chacun de tirer pleinement parti des possibilités offertes par les nouvelles technologies pour accéder aux services publics et les utiliser, en surmontant les divisions et l'exclusion sociales et économiques.**

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

L'inclusion et l'accessibilité doivent faire partie de l'ensemble du cycle de développement d'un service public béninois en termes de conception, de contenu de l'information et de diffusion. Il devrait être conforme aux spécifications d'e-accessibilité reconnues au niveau international.

L'inclusion et l'accessibilité impliquent généralement une diffusion multicanale. La fourniture traditionnelle de services sur papier ou en face à face peut devoir coexister avec la livraison 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 incapables, de manière permanente ou temporaire, d'utiliser directement les services publics.

RECOMMANDATION 27
Les administrations publiques doivent s'assurer que tous les sites Web et services publics du secteur public sont accessibles à tous les citoyens, y compris aux personnes handicapées et ayant des besoins spéciaux.

RECOMMANDATION 28
Les interfaces des systèmes d'information, des sites Web et des services du secteur public béninois doivent être au moins conformes aux directives pour l'accessibilité aux contenus Web (WCAG)[3] critères de qualité - niveau AA.

RECOMMANDATION 29
Les institutions du secteur public DOIVENT fournir des informations dans des formats ouverts. Les citoyens ne doivent pas engager de dépenses supplémentaires pour utiliser les informations (par exemple, obtenir leur propre logiciel).

◆ SÉCURITÉ ET CONFIDENTIALITÉ

Les citoyens et les entreprises doivent avoir la certitude que, lorsqu'ils interagissent avec les autorités publiques, ils le font dans un environnement sûr et digne de confiance et en pleine conformité avec les réglementations en vigueur. Les administrations publiques doivent garantir la vie privée des citoyens et la confidentialité, l'authenticité, l'intégrité et la non-répudiation des informations fournies par les citoyens et les entreprises.

Dans le cadre des contraintes de sécurité nécessaires, **les citoyens et les entreprises ont le droit de vérifier les informations que les administrations ont collectées à leur sujet et de décider si ces informations**

peuvent être utilisées à des fins autres que celles pour lesquelles elles avaient été fournies à l'origine.

RECOMMANDATION 30
Le Bénin doit définir un cadre commun de sécurité et de protection de la vie privée et établir des processus pour les services publics afin de garantir un échange de données sécurisé et fiable entre les administrations publiques et dans les interactions avec les citoyens et les entreprises.

RECOMMANDATION 31
Les systèmes d'information béninois doivent garantir la confidentialité, l'intégrité, l'authenticité, la disponibilité et le caractère vérifiable des données et des services.

RECOMMANDATION 32
Les citoyens doivent bénéficier de services grâce auxquels ils peuvent vérifier et, si nécessaire, corriger les données collectées à leur sujet par le secteur public.

RECOMMANDATION 33
Les citoyens doivent bénéficier de services grâce auxquels ils découvrent qui, et à quelles fins, a utilisé les données collectées à leur sujet dans le secteur public.

RECOMMANDATION 34
Les interfaces utilisateur des services doivent être fournies en plus du français, également en anglais ou dans toute autre langue pertinente pour les utilisateurs.

RECOMMANDATION 35
La langue par défaut doit être le français pour les interfaces utilisateur des systèmes d'information créés pour les résidents du Bénin.

RECOMMANDATION 36
Les interfaces utilisateur des systèmes d'information doivent être facilement adaptables à d'autres langues à l'aide de fichiers de traduction.

◆ MULTILINGUISME

Le multilinguisme et la neutralité linguistique entrent en jeu non seulement au niveau des interfaces utilisateur, mais à tous les niveaux de la 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.

2.3.4. Principes de base de la coopération entre administrations publiques

◆ SIMPLIFICATION ADMINISTRATIVE

Dans la mesure du possible, **les administrations publiques doivent chercher à rationaliser et simplifier leurs processus administratifs en les améliorant ou en éliminant ceux qui n'offrent aucune valeur publique.** La simplification administrative peut aider les entreprises et les citoyens à réduire le fardeau administratif lié au respect de la législation ou des obligations. De même, les administrations publiques devraient introduire des services utilisant des moyens électroniques, y compris leurs interactions avec les autres administrations publiques, les citoyens et les entreprises.

La dématérialisation des services publics devrait s'effectuer conformément aux concepts suivants :

- **numérique par défaut,** le cas échéant, afin qu'il y ait au moins un canal numérique disponible pour accéder à et utiliser un service public béninois donné ;
- **digital-first,** ce qui signifie que la priorité est donnée à l'utilisation de services publics via des canaux numériques, tout en appliquant le concept de distribution multicanaux et la politique d'interdiction de porte, c'est-à-dire que les canaux physiques et numériques coexistent.

RECOMMANDATION 37
Les administrations doivent simplifier les processus et utiliser les canaux numériques chaque fois que cela est approprié pour la fourniture de services publics, répondre rapidement et avec une qualité élevée aux demandes des utilisateurs et réduire le fardeau administratif des administrations publiques, des entreprises et des citoyens.

◆ CONSERVATION DE L'INFORMATION

La législation exige que les décisions et les données soient stockées et accessibles pendant un temps déterminé. Cela signifie que **les archives et les informations sous forme électronique détenues par les administrations publiques à des fins de documentation des procédures et des décisions doivent être préservées et converties, le cas échéant, en 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, dans le respect des dispositions de sécurité et de confidentialité.

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

RECOMMANDATION 38
Le Bénin doit formuler une politique de préservation à long terme des informations.

◆ ÉVALUATION DE L'EFFICACITÉ ET DE L'EFFICIENCE

L'administration publique devrait **veiller à ce que les solutions servent les entreprises et les citoyens de la manière la plus efficace et la plus efficiente et offrent le meilleur rapport qualité-prix pour l'argent des**

RECOMMANDATION 39

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

contribuables. Il existe de nombreuses façons de prendre en compte la valeur des services interopérables, notamment 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 doivent être évaluées lorsque l'on s'efforce d'assurer l'efficacité et l'efficience d'un service public béninois.

2.4. Identification et sélection des normes

Les normes et spécifications sont fondamentales pour l'interopérabilité. Il y a six étapes pour les gérer correctement :

- **identifier les normes et spécifications candidates** en fonction des besoins et des exigences spécifiques ;
- **évaluer les normes et spécifications candidates** à l'aide de méthodes normalisées, transparentes, équitables et non discriminatoires ;
- **mettre en œuvre les normes et spécifications** conformément aux plans et directives pratiques ;
- **contrôler le respect des normes et spécifications ;**
- **gérer le changement** avec des procédures appropriées ;
- **documenter des normes et spécifications,** dans des catalogues ouverts, à l'aide d'une description normalisée.

RECOMMANDATION 40

La structure de coordination devrait mettre en place des processus permettant de sélectionner les normes et spécifications pertinentes, de les évaluer, de surveiller leur mise en œuvre, de vérifier leur conformité et de tester leur interopérabilité.

Les principes et la structure des normes du secteur public et des normes convenues ont été définis dans le processus de construction de la solution d'interopérabilité du Bénin. Le présent document fournit la liste des décisions les plus pertinentes concernant les normes ouvertes. Le secteur public approuve, sur la base des recommandations du groupe de travail sur les normes ouvertes et en coopération avec les autres parties concernées, un ensemble minimal de normes ouvertes du secteur public, dont le respect est obligatoire pour le secteur public. Le choix et l'évaluation des normes sont publics et équilibrés.

Ci-dessous une liste des normes ouvertes les plus pertinentes, que les institutions devraient utiliser pour communiquer entre elles et avec le public sur des sites web et dans des bases de données publiques. En ce qui concerne la communication interne, les institutions sont autorisées, bien que cela ne soit pas recommandé, à utiliser d'autres normes.

- **CSV (valeurs séparées par des virgules [.csv]) –** format indépendant de la plate-forme pour la soumission des données de feuille[4]
- **HTML (HyperText Markup Language [.html]) –** langage de balisage hypertexte pour la création de documents Web[5]
- **ASiC (Associated Signature Container est la norme ETSI TS 102 918 v 1.1.1 (2011-04))** de l'ETSI pour la signature numérique ou une norme plus concrète comme BDOC[6]
- **CSS (langage de feuilles de style en cascade)**[7]
- **JPEG (Joint Photographic Experts Group [.jpg]) –** format graphique[8]
- **Information géographique :**
  - ISO 19115 : 2003 « Information géographique - Métadonnées »
  - ISO / TS 19139 : 2007 « Information géographique - Métadonnées - Implémentation d'un schéma XML »
- **GZIP –** format du paquet[9]
- **MPEG (Moving Picture Experts Group [.mpeg]) –** format vidéo[10]
- **ODF (Open Document Format [.odf]) –** format de document ouvert pour applications bureautiques[11] ;
- **Les sous-formats ODF :**
  - .odb (base de données)
  - .odf (formule)
  - .odg (dessin)
  - .odp (présentation)
  - ods (feuilles de calcul)
  - .odt (textes)
- **PDF (Portable Document Format [.pdf]) –** format de document indépendant de la plateforme
- **PDF / a (format de document portable / archive)**[12] **–** format d'archivage des fichiers .pdf
- **SOAP (Simple Object Access Protocol)** est une spécification de pro-

tocole permettant d'échanger des informations structurées lors de la mise en œuvre de services Web dans des réseaux informatiques.

- **PNG (Portable Network Graphics [.png]) –** format graphique raster[13]
- **SVG (Scalable Vector Graphi c [.svg]) –** format de graphique vectoriel[14]
- **TIFF (format de fichier d'image marquée [.tif]) –** format graphique raster[15]
- **TXT (Texte brut, fichier texte [.txt]) –** format de texte brut non traité
- **XAdES (signatures électroniques avancées XML) –** y compris les normes :
  - ETSI TS 101 903 signatures électroniques avancées XML
  - ETSI TS 103 171 Profil de base XAdES
  - ETSI TS 102 918 Containers Signature associés
  - ETSI TS 103 174 AsiC Profile de base
- **XML (Langage de balisage hypertexte extensible [.xml]) –** Langage de balisage hypertexte[16]
- **XSL (langage de style extensible)**[17]
- **WSAG (Directives pour l'accessibilité aux contenus Web)**[18]
- **WSDL (langage de description de services Web)**[19] **–** un langage de définition d'interface basé sur XML utilisé pour décrire les fonctionnalités offertes par un service Web

RECOMMANDATION 41
Les administrations doivent respecter un ensemble minimal convenu de normes ouvertes.

3 ◆ MODÈLE CONCEPTUEL POUR LA FOURNITURE DE SERVICES PUBLICS INTÉGRÉS

3.1. Introduction

Ce chapitre propose un modèle conceptuel pour les services publics intégrés. **Il est pertinent pour tous les niveaux de gouvernement : local, gouvernemental, ministériel, national. Le modèle est modulaire et comprend des composants de service faiblement couplés interconnectés via une infrastructure partagée.**

Les administrations publiques doivent identifier, négocier et s'entendre sur une approche commune pour l'interconnexion des composants de service. Cela se fera à différents niveaux administratifs en fonction de la structure organisationnelle. Les limites d'accès aux services et aux informations DEVRAIENT être définies à l'aide d'interfaces et de conditions d'accès.

Il existe des solutions techniques bien connues et largement utilisées, telles que des services web, mais leur mise en œuvre au niveau de l'État nécessitera des efforts concertés des administrations publiques, notamment des modèles, normes et accords communs ou compatibles sur des infrastructures communes.

RECOMMANDATION 42
Utiliser le modèle conceptuel pour concevoir de nouveaux services ou pour restructurer des services existants et pour réutiliser, chaque fois que possible, les composants de service et de données existants.

RECOMMANDATION 43
Le Bénin doit décider d'un système commun d'interconnexion des composants de service faiblement couplés, mettre en place et entretenir l'infrastructure nécessaire pour établir et maintenir des services publics au niveau de l'État.

3.2. Aperçu du modèle

Le modèle conceptuel promeut l'idée de l'interopérabilité par conception. Cela signifie que pour que les services publics béninois soient interopérables, ils doivent être conçus conformément au modèle proposé et en tenant compte de certaines exigences en matière d'interopérabilité et de réutilisa-

bilité. Le modèle préconise la réutilisabilité en tant que moteur de l'interopérabilité, en reconnaissant que les services publics béninois doivent réutiliser les informations et les services existants et susceptibles d'être disponibles à partir de diverses sources à l'intérieur ou au-delà des limites organisationnelles des administrations publiques. Les informations et les services devraient être récupérables et disponibles dans des formats interopérables.

Les composants de base du modèle conceptuel sont présentés ci-après.

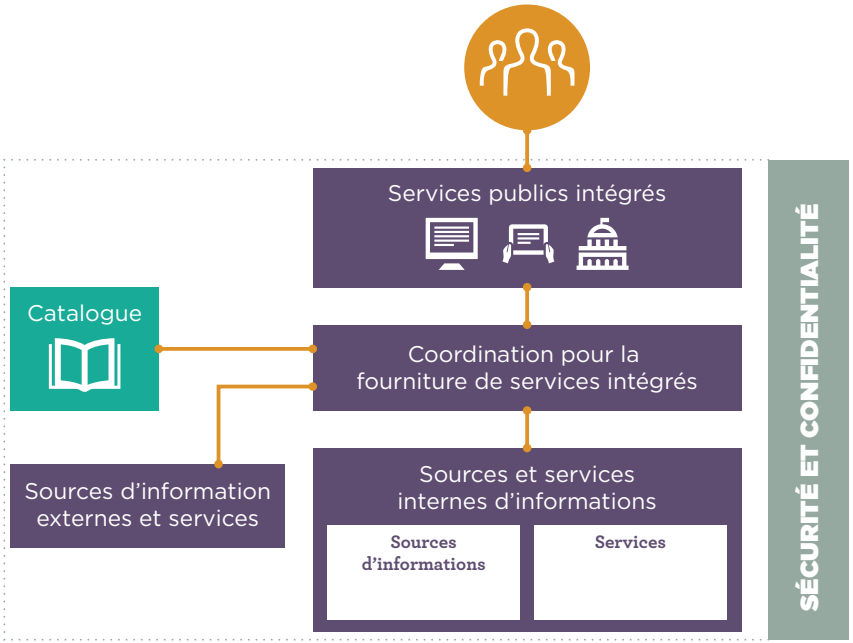


Figure 1 Modèle conceptuel pour les services publics intégrés

La structure du modèle comprend :

- **« Prestation de services intégrée » basée sur une « fonction de coordination »** destinée à éliminer la complexité pour l'utilisateur final ;
- **Une politique de fourniture de services** offrant des options et des canaux alternatifs pour la fourniture de services, tout en garantissant la disponibilité des canaux numériques (numérique par défaut) ;
- **Réutilisation des données et des services** pour réduire les coûts et augmenter la qualité et l'interopérabilité des services ;
- **Des catalogues décrivant les services réutilisables** et autres éléments d'actif afin d'accroître leur facilité de recherche et d'utilisation ;
- **Gouvernance intégrée de la fonction publique ;**
- **Sécurité et confidentialité.**

3.3. Fonction de coordination

La fonction de coordination veille à ce que les besoins soient identifiés et les services appropriés invoqués et / ou coordonnés pour fournir un service public. Cette fonction devrait 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 service public intégrée » et sont exécutées par la fonction de coordination.

- **1. Identification du besoin :** elle est provoquée par une demande de service public émanant d'un citoyen ou d'une entreprise.
- **2. Planification :** Cela implique d'identifier les services et les sources d'informations nécessaires, d'utiliser les catalogues disponibles et de les regrouper en un processus unique, en tenant compte des besoins spécifiques des utilisateurs (par exemple, la personnalisation).
- **3. Exécution :** il s'agit de collecter et d'échanger des informations, d'appliquer des règles commerciales (conformément à la législation et aux politiques en vigueur) pour accorder ou refuser l'accès à un service, puis de fournir le service demandé aux citoyens ou aux entreprises.
- **4. Évaluation :** après la fourniture du service, les commentaires des utilisateurs sont recueillis et évalués.

3.4. Sources d'information internes et services

Les administrations publiques produisent et mettent à disposition un grand nombre de services, tandis qu'elles gèrent et maintiennent un grand nombre et une grande variété de sources d'informations. Ces sources d'informations sont souvent inconnues en dehors des limites d'une administration particulière (et parfois même à l'intérieur de ces limites). Il en résulte une duplication des efforts et une sous-exploitation des ressources disponibles et des solutions.

Les sources d'information (registres de base, portails de données ouvertes et autres sources d'information faisant autorité) et les services

RECOMMANDATION 44

Développer une infrastructure partagée de services réutilisables et de sources d'informations pouvant être utilisées par toutes les autres administrations publiques.

disponibles non seulement à l'intérieur du système administratif mais également dans l'environnement externe peuvent être utilisés pour créer des services publics intégrés constitutifs.

Les blocs de construction (sources d'information et services) devraient rendre leurs données ou fonctionnalités accessibles en utilisant des approches orientées services.

Les administrations publiques doivent promouvoir des politiques de partage des services et des sources d'information de trois manières principales :

- **1. Réutilisation :** lors de la conception de nouveaux services ou de la révision de services existants, la première étape consiste à déterminer si les services et les sources d'information existants peuvent être réutilisés ;
- **2. Publication :** lors de la conception de nouveaux services et sources d'information ou de la révision de services existants, les services et sources d'information réutilisables devraient être mis à la disposition de tiers pour être réutilisés ;
- **3. Agrégation :** une fois les services et les sources d'informations appropriés identifiés, vous devez les agréger pour former un processus intégré de fourniture de services. Les blocs de construction doivent présenter une capacité native de combinaison (« interopérabilité par conception ») pour être prêts à être mélangés dans différents environnements avec un minimum de personnalisation. Cette agrégation concerne les informations, les services et d'autres solutions d'interopérabilité (par exemple, les logiciels).

L'approche par blocs de construction réutilisables trouve une application appropriée en mappant des solutions aux blocs de construction conceptuels d'une architecture de référence. Cela permet de détecter les composants réutilisables, ce qui favorise également la rationalisation. Le résultat de cette cartographie est une cartographie de solutions, y compris leurs éléments de base, qui PEUVENT être réutilisés pour répondre aux besoins commerciaux courants et assurer l'interopérabilité.

Plus précisément, afin d'éviter les doubles emplois, les coûts supplémentaires et les problèmes d'interopérabilité tout en augmentant la qualité des services offerts, le modèle conceptuel propose deux types de réutilisation :

- **Réutilisation des services :** différents types de services peuvent être réutilisés. Les exemples incluent les services publics de base, par exemple la délivrance d'un acte de naissance, et les services partagés tels que l'identification électronique et la signature électronique. Les services partagés peuvent être fournis par le secteur public, le secteur privé ou selon des modèles de partenariat public-privé (PPP) ;
- **Réutilisation des informations :** les administrations publiques stockent déjà de grandes quantités d'informations susceptibles d'être réutilisées. Les exemples incluent : les données de base des registres de base en tant que données faisant autorité, utilisées par plusieurs applications et systèmes ; données ouvertes sous licences à usage ouvert publiées par des organismes publics ; d'autres types de données faisant autorité validées et gérées sous l'égide d'autorités publiques. Les registres de base et les données ouvertes sont traités plus en détail dans la section suivante.

3.5. Registres de base

Les registres de base sont la pierre angulaire de la prestation des services publics béninois. **Un registre de base est une source d'informations fiable et faisant autorité, qui PEUT et DEVRAIT être réutilisée numériquement par d'autres, dans laquelle une organisation est responsable de la collecte, de l'utilisation, de la mise à jour et de la conservation des informations.** Les registres de base sont des sources fiables d'informations de base sur des éléments de données tels que des personnes, des sociétés, des véhicules, des permis, des bâtiments, des emplacements et des routes. Ce type d'information constitue les « données de base » pour les administrations publiques et la prestation de services publics béninois. « Autoritaire » signifie ici qu'un registre de base est considéré comme la « source » d'informations, c'est-à-dire qu'il indique l'état correct, qu'il est à jour et qu'il présente la plus haute qualité et intégrité possible.

Dans le cas des registres de base, une seule entité organisationnelle est responsable de la qualité des données et de la mise en place de mesures

RECOMMANDATION 45

Mettre à la disposition des tiers des sources d'information faisant autorité, tout en mettant en œuvre des mécanismes d'accès et de contrôle permettant de garantir la sécurité et la confidentialité conformément à la législation applicable.

RECOMMANDATION 46

Développer des interfaces avec les registres de base et les sources d'information faisant autorité, publier les moyens sémantiques et techniques ainsi que la documentation nécessaire pour que d'autres puissent se connecter et réutiliser les informations disponibles.

pour garantir leur exactitude. **Ces registres sont sous le contrôle légal des administrations publiques, tandis que leur fonctionnement et leur maintenance PEUVENT être sous-traités à d'autres organisations si nécessaire.** Il existe plusieurs types de registres de base, par exemple population, entreprises, véhicules, cadastres, etc. Pour les administrations, il est important d'obtenir une vue d'ensemble des opérations des registres de base et des données qu'elles stockent (un registre de registres).

Dans le cas de registres distribués, il doit y avoir une seule entité organisationnelle responsable de chaque partie du registre. De plus, une seule entité doit être responsable de la coordination de toutes les parties du registre distribué.

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

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

L'intendant des informations est l'organe (ou éventuellement l'individu) responsable de la collecte, de l'utilisation, de la mise à jour, de la maintenance et de la suppression des informations. Cela inclut la définition de l'utilisation autorisée des informations, le respect des règles de confidentialité et des politiques de sécurité, la garantie que les informations sont à jour et l'accessibilité des données aux utilisateurs autorisés.

Les registres de base doivent élaborer et mettre en œuvre un plan d'assurance de la qualité des données afin d'assurer la qualité de leurs données. Les citoyens et les entreprises doivent pouvoir vérifier l'exactitude, la précision et l'exhaustivité de leurs données contenues dans les registres de base.

Un guide de la terminologie utilisée et / ou un glossaire des termes pertinents utilisés dans chaque base de registre doit être mis à la disposition des utilisateurs, que ce soit à des fins d'information ou de lecture.

RECOMMANDATION 47

Associer à chaque registre de base les métadonnées appropriées, notamment la description de son contenu, l'assurance de service et les responsabilités, le type de données de base qu'elle conserve, les conditions d'accès, les licences correspondantes, une terminologie, un glossaire et des informations sur les données de base les contenant et qu'il utilise à partir d'autres registres de base.

RECOMMANDATION 48

Créer et suivre des plans d'assurance qualité des données pour les registres de base et les données de base correspondantes.

3.6. Données ouvertes

La loi béninoise sur l'information du secteur public fournit un cadre juridique commun pour la réutilisation des données du secteur public. L'accent est mis sur la publication de données lisibles par machine à l'usage de tiers pour stimuler la transparence, une concurrence loyale, l'innovation et une économie axée sur les données. **Pour assurer des conditions équitables, l'ouverture et la réutilisation des données DOIVENT être non discriminatoires, ce qui signifie que les données doivent être interopérables pour pouvoir être trouvées, découvertes et traitées.**

Il existe actuellement de nombreux obstacles à l'utilisation des données ouvertes. Il est souvent publié sous différentes formes ou dans différents formats qui empêchent une utilisation facile, il peut manquer de métadonnées appropriées, les données elles-mêmes peuvent être de faible qualité, etc. L'idéal serait que les métadonnées de base et la sémantique des ensembles de données ouverts DEVRAIENT être décrites dans un format standard lisible par les machines.

Les données peuvent être utilisées de différentes manières et à différentes fins. La publication de données ouverte devrait permettre cela. Néanmoins, les utilisateurs peuvent rencontrer des problèmes avec les jeux de données, commenter leur qualité ou préférer d'autres méthodes de publication. Les boucles de rétroaction peuvent aider à 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, l'interopérabilité et la sécurité juridiques sont essentielles. Pour cette raison, le droit de chacun de réutiliser des données ouvertes devrait être clairement communiqué dans l'ensemble des États

RECOMMANDATION 49

Établir des procédures et des processus pour intégrer l'ouverture de données dans les processus opérationnels communs des administrations, leurs routines de travail et dans le développement de nouveaux systèmes d'information.

RECOMMANDATION 50

Publier les données ouvertes dans des formats non-propriétaires lisibles par machine. Veiller à ce que les données ouvertes soient accompagnées de métadonnées de haute qualité lisibles par machine dans des formats non-propriétaires, comprenant une description de leur contenu, le mode de collecte des données, son niveau de qualité et les conditions de licence selon lesquelles elles sont mises à disposition. L'utilisation de vocabulaires communs pour l'expression de métadonnées est recommandée.

RECOMMANDATION 51

Communiquer clairement le droit d'accéder aux données ouvertes et de les réutiliser. Les régimes juridiques visant à faciliter l'accès et la réutilisation, tels que les licences, doivent être normalisés autant que possible.

membres, et les régimes juridiques visant à faciliter la réutilisation de données, tels que les licences, devraient autant que possible être promus et uniformisés.

3.7. Catalogues

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

RECOMMANDATION 52

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

3.8. Sources d'information et services externes

Les administrations publiques doivent exploiter les services fournis par des tiers en dehors de leurs frontières organisationnelles, tels que les services de paiement fournis par des institutions financières ou les services de connectivité fournis par des fournisseurs de télécommunications. Ils doivent également exploiter des sources d'informations 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 collectées via l'Internet des objets (capteurs, par exemple) et des applications de réseau social.

RECOMMANDATION 53

Dans la mesure où cela est utile et réalisable, les administrations publiques devraient utiliser des sources d'information et des services externes lors du développement des services publics béninois.

3.9. Sécurité et confidentialité

La sécurité et la confidentialité sont des préoccupations primordiales dans la fourniture de services publics. Les administrations publiques devraient s'assurer que :

- **elles respectent l'approche de la protection de la vie privée** et de la sécurité dès la conception pour sécuriser l'ensemble de leur infrastructure et leurs blocs de construction ;
- **les services ne sont pas vulnérables aux attaques** susceptibles d'interrompre leur fonctionnement et de causer le vol ou l'endommagement des données ;
- **elles respectent les exigences et obligations légales en matière de protection des données et de la vie privée,** tout en reconnaissant les risques pour la vie privée résultant du traitement et de l'analyse avancés des données.

Elles veillent également à ce 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 impact potentiel et planifier les réponses à l'aide de mesures techniques et organisationnelles appropriées. Sur la base des dernières évolutions technologiques, ces mesures doivent garantir que le niveau de sécurité correspond au degré de risque ;
- **des « Plans de continuité des activités » et « plans de sauvegarde et de reprise » pour mettre en place les procédures** nécessaires au fonctionnement des fonctions après un événement désastreux et ramener toutes les fonctions à la normale le plus tôt possible ;
- **un « plan d'accès et d'autorisation des données » qui détermine qui a accès à quelles données et dans quelles conditions,** afin de garantir la confidentialité. Les accès non autorisés et les violations de la sécurité doivent être surveillés et des actions appropriées doivent être prises pour éviter toute répétition d'infractions ;
- **utilisation de services de confiance qualifiés** pour assurer l'intégrité, l'authenticité, la confidentialité et la non-répudiation des données.

Lorsque des administrations publiques et d'autres entités échangent des informations officielles, celles-ci doivent être transférées, en fonction des exigences de sécurité, via une couche sécurisée d'échange de données sécurisée, harmonisée, gérée et contrôlée. Les mécanismes de transfert devraient faciliter les échanges d'informations entre les administrations, les entreprises et les citoyens :

- **enregistré et vérifié,** de sorte que l'expéditeur et le destinataire aient été identifiés et authentifiés selon les procédures et mécanismes convenus ;
- **crypté,** de sorte que la confidentialité des données échangées soit assurée ;
- **horodaté,** pour maintenir l'heure exacte du transfert et de l'accès aux enregistrements électroniques ;
- **journalisé,** pour que les enregistrements électroniques soient archivés, assurant ainsi une piste d'audit légale.

Des mécanismes appropriés doivent :

- **permettre un échange sécurisé de messages, enregistrements, formulaires et autres types d'informations** vérifiés électroniquement entre les différents systèmes ;
- **gérer les exigences de sécurité spécifiques** et les services d'identification électronique et de confiance tels que la création et la vérification de signatures / cachets électroniques ;
- **surveiller le trafic pour détecter les intrusions,** les changements de données et tout autre type d'attaque.

Les informations doivent également être protégées de manière appropriée pendant la transmission, le traitement et le stockage par différents processus de sécurité tels que :

- **définir et appliquer des politiques de sécurité ;**
- **la formation et la sensibilisation** à la sécurité ;
- **la sécurité physique** (y compris contrôle d'accès) ;
- **la sécurité dans le développement ;**
- **la sécurité des opérations** (y compris surveillance de la sécurité, gestion des incidents, gestion des vulnérabilités) ;
- **les revues de sécurité** (y compris audits et vérifications techniques).

Des exigences communes pour la protection des données doivent être convenues avant de fournir des services agrégés.

La fourniture d'un échange de données sécurisé nécessite également plusieurs fonctions de gestion, notamment :

- **la gestion des services pour superviser toutes les communications d'identification, d'authentification, d'autorisation, de transport de données, etc.,** y compris les autorisations d'accès, la révocation et l'audit ;
- **l'enregistrement de service pour fournir, sous réserve d'une autorisation en bonne et due forme, l'accès aux services disponibles** par le biais d'une localisation préalable et d'une vérification de la fiabilité du service ;
- **la consignation des services** pour garantir que tous les échanges de données sont consignés pour une référence future et archivés si nécessaire.

RECOMMANDATION 54

Prendre en compte les exigences spécifiques en matière de sécurité et de confidentialité et identifier les mesures prévues par la structure de coordination pour la fourniture de chaque service public conformément aux plans de gestion des risques.

RECOMMANDATION 55

Utiliser les services de confiance prévus par la structure de coordination comme mécanismes assurant des échanges de données sécurisés et protégés dans les services publics.

4 ◆ ARCHITECTURE D'INTEROPÉRABILITÉ

4.1. Concepts clés

L'architecture d'interopérabilité est une architecture de référence pour le développement de solutions d'administration en ligne pour le Bénin. L'architecture d'interopérabilité décrit les principes d'architecture et fournit une architecture de référence conceptuelle pour la mise en place du e-gouvernement au Bénin. Une architecture de référence conceptuelle définit la structure des composants conceptuels, leurs relations réciproques, ainsi que les principes et directives régissant leur conception et leur évolution dans le temps.

◆ PRINCIPE « UNE SEULE FOIS »

Le modèle proposé repose sur 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 les mêmes informations.** Selon le principe « une seule fois », les structures de l'Administration doivent prendre des mesures pour partager des données entre eux, dans le respect des règles de confidentialité et de protection des données. Cela nécessite une solution générique et évolutive pour interconnecter différents systèmes. Les données ne sont conservées que dans une base de données, où elles servent de données de base. Les exigences de disponibilité peuvent conduire à la copie de données, mais il faut, le cas échéant, tenir compte du fait que les données peuvent être obsolètes.

◆ SOCIÉTÉ EN TANT QU'ORGANISATION CENTRÉE SUR LE SERVICE

Toutes les activités des fonctionnaires, des entrepreneurs, des citoyens et des applications ou systèmes d'information sont considérées comme des services. Les utilisateurs finaux voient les services dans une salle de service commune. Ils ne sont pas intéressés par l'organisation qui fournit le service, mais par le service lui-même. Bien que les secteurs privé et public agissent selon des règles commerciales assez différentes, les utilisateurs de leurs services sont les mêmes. Il est donc pratique que les secteurs privé et public développent et gèrent les services conjointement.

◆ SÉPARATION DES SYSTÈMES « FRONT-END » ET « BACK-END »

Dans les systèmes d'information du secteur public, les systèmes frontaux et dorsaux doivent être 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 dorsaux est la gestion des données et la fourniture de services réseau ; ils ne traitent pas d'authentification et d'autorisation. Par conséquent, il n'est pas nécessaire de créer des composants d'authentification et d'autorisation de l'utilisateur final dans les systèmes principaux. **Les services Web des systèmes principaux ne sont disponibles que pour l'utilisateur final par le biais d'intermédiaires de services (systèmes font-end).**

◆ RÉUTILISATION DES COMPOSANTS

Un modèle de service complet basé sur des composants pour les administrations publiques permet **la création de services publics en réutilisant autant que possible les composants de service existants. Les administrations publiques DOIVENT s'entendre sur un système commun pour interconnecter des composants faiblement couplés et mettre en place l'infrastructure nécessaire.**

◆ ARCHITECTURE ORIENTÉE SERVICE

Dans l'élaboration de l'architecture informatique d'état, les principes de l'architecture SOA (architecture orientée service – ou Service Oriented Architecture en anglais) DOIVENT être suivis. Dans le cas d'une architecture orientée service, différents systèmes fournissent divers services d'information via les « interfaces de service », qui peuvent être utilisées par d'autres systèmes d'information. Les descriptions de ces interfaces doivent contenir **suffisamment d'informations pour l'identification et l'utilisation d'un service sans que le système qui utilise le service n'ait à se préoccuper de l'architecture interne, la plate-forme, etc. du système fournissant le service.** En cas de SOA, l'éditeur de services et le réel fournisseur de services ne doivent pas nécessairement être les mêmes, bien 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 la SOA.

◆ LIAISON DES PROCESSUS MÉTIER VIA DES SERVICES AGRÉGÉS

Les systèmes d'information communiquent entre eux via des services agrégés. Si, pour l'exécution d'un processus métier dans une structure

donnée, des données sont nécessaires ou un flux de travail doit être exécuté dans une autre structure, des services agrégés sont utilisés. **Les structures de l'Administration doivent s'assurer que les données et les services qu'elles offrent puissent être utilisés en tant que services agrégés.** Les services globaux ou complexes sont combinés à partir de services de base fiables (par exemple, les résultats d'un service de base sont utilisés comme entrées pour d'autres). L'utilisateur perçoit un service complexe comme un seul service. Dans le cas de services globaux, une attention particulière doit être accordée aux risques liés à la sécurité, aux droits d'utilisation de service, ainsi qu'au danger de combinaison de données.

RECOMMANDATION 56

Les structures de l'Administration doivent construire une solution interopérable en suivant les principes architecturaux convenus.

◆ ÉVITER LE « POINT DE DÉFAILLANCE UNIQUE »

Il est recommandé **d'utiliser des solutions dans lesquelles la panne d'une partie du système peut perturber le fonctionnement de l'ensemble du système.**

4.2. Services d'infrastructure

L'infrastructure d'interopérabilité représente un ensemble de systèmes informatiques prenant en charge la fourniture de services publics béninois aux administrations, aux citoyens et aux entreprises. Un composant du système peut être de nature technique (moteur de workflow, module d'authentification, registre de service, par exemple) mais également fonctionnel (méthodologie, modèle, etc.). Il existe deux types de services à savoir les services métiers et les services d'infrastructure. Un service d'infrastructure est une fonctionnalité technique générique d'un système prenant en charge la fourniture d'un ou de plusieurs services métiers. Les services d'infrastructure sont masqués pour les utilisateurs finaux.

L'architecture d'interopérabilité du Bénin suit le principe orienté service. Cela signifie que toutes les activités d'une organisation sont des services. Le service peut être :

- **une activité récurrente ;**
- **un élément de comportement** fournissant des fonctionnalités spécifiques en réponse aux demandes d'acteurs ou d'autres services.

Une vue de haut niveau de l'architecture d'interopérabilité béninoise est décrite à la figure 2. Cette vue de haut niveau 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 vision des principes** sous-jacents du cadre d'interopérabilité béninois.

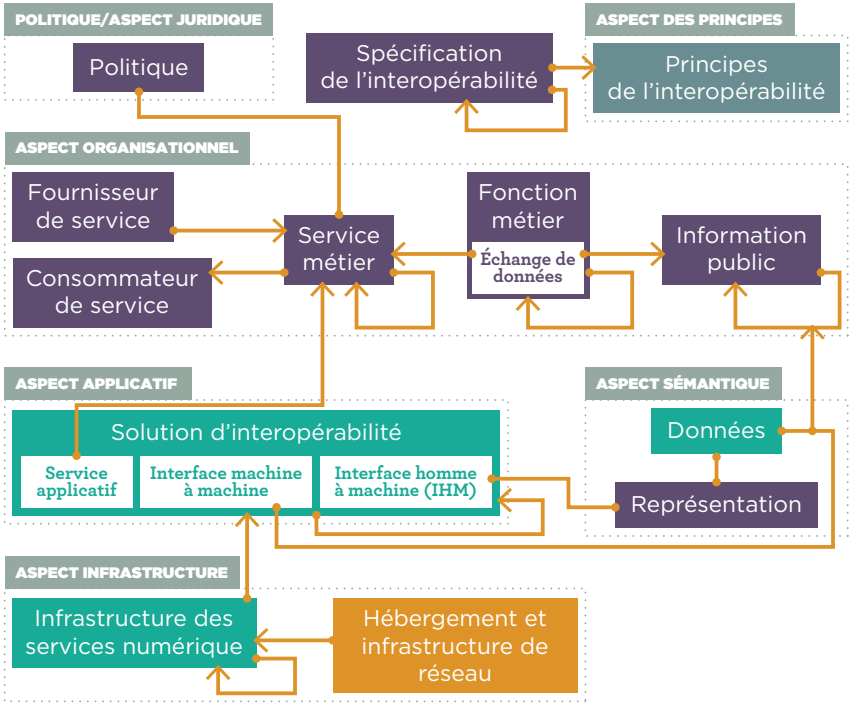


Figure 2 : Vue de haut niveau des services

Afin de garantir l'interopérabilité des systèmes d'information du secteur public, celui-ci développera et mettra en œuvre plusieurs composantes d'infrastructure communes. Les composants les plus importants (ou catalyseurs) de l'infrastructure béninoise d'administration en ligne sont :

- **l'écosystème sécurisé d'échange de données ;**
- **l'écosystème eID et services de confiance ;**
- **le catalogue des solutions d'interopérabilité (CatIS) ;**
- **l'infrastructure Open Data ;**

› **le point de contact uniques pour les services.**

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

RECOMMANDATION 57

Pour réaliser l'interopérabilité, le gouvernement doit développer des services d'infrastructure communs disponibles pour toutes les administrations, les entreprises et les citoyens.

RECOMMANDATION 58

Les services d'infrastructure doivent être gratuits pour les administrations, les entreprises et les citoyens.

4.3. L'écosystème d'échange de données sécurisé

Tout échange de données doit se faire de manière sécurisée et contrôlée. Le bloc fonctionnel d'échange de données sécurisé est le facteur le plus crucial pour la mise en œuvre du modèle.

Dans les systèmes d'information du secteur public, les systèmes front-end et back-end sont clairement séparés sur le plan architectural. Les systèmes back-end sont tous des registres et bases de données du secteur public. La tâche des systèmes dorsaux est la gestion des données et la fourniture de services réseau. Ils ne traitent pas d'authentification et d'autorisation. Par conséquent, il n'est pas nécessaire d'intégrer dans les systèmes dorsaux des composants d'authentification et d'autorisation de l'utilisateur final. Les services réseau des systèmes dorsaux sont mis à la disposition de l'utilisateur final uniquement par le biais d'intermédiaires de services (systèmes front-end).

RECOMMANDATION 59

Les systèmes dorsaux et front-end doivent être séparés sur le plan architectural.

RECOMMANDATION 60

Les systèmes back-end ne doivent pas être impliqués dans l'authentification et l'autorisation de l'utilisateur final.

RECOMMANDATION 61

Les services des systèmes dorsaux doivent être disponibles pour un utilisateur final uniquement via des systèmes front-end.

Les systèmes front-end sont divisés en systèmes internes (par exemple, intranet) et publics. Les systèmes front- end internes sont chargés d'administrer les droits de l'accès de leurs employés à tout service ayant une valeur probante dans le pays. Les droits d'utilisation de service sont personnels et des restrictions peuvent y être ajoutées (par exemple, limite de temps pour l'utilisation d'un service). Les systèmes front-end ne doivent pas octroyer de droits aux employés d'autres institutions. Les certificats qualifiés sont utilisés pour l'autorisation de services ayant une valeur probante.

La sécurité est une préoccupation essentielle pour le partage de données et la fourniture de services publics. Les administrations publiques fournissant des services publics doivent garantir que :

› **l'infrastructure complète et les blocs de construction sont sécurisés** en respectant les principes de l'approche de la protection de la vie privée dès la conception ;

› **les services ne sont pas vulnérables aux attaques** pouvant en interrompre le fonctionnement, provoquer le vol ou l'endommagement de données ;

› **les services respectent les exigences et obligations légales** en matière de protection des données et de la vie privée.

Les mécanismes de partage de données doivent faciliter l'échange d'informations entre les administrations, les entreprises et les citoyens :

› **enregistré et vérifié :** l'expéditeur et le destinataire ont été identifiés et authentifiés selon les procédures et mécanismes convenus ;

› **crypté :** la confidentialité des données échangées est assurée ;

› **horodaté :** maintenir l'heure exacte ;

› **enregistré :** les enregistrements électroniques sont enregistrés et archivés pour assurer un suivi légal.

La figure 3 ci-dessous illustre la vue logique des composants d'infrastructure de services sécurisés de la plate- forme de partage de données du gouvernement et de leur interconnexion.

L'échange de données sécurisé est basé sur les réseaux TCP/IP. Les systèmes d'information sont de deux types :

› **les fournisseurs de services** (éditeurs, back-end) ;

› **les consommateurs** (abonnés, front-end).

Un système d'information peut jouer simultanément les deux rôles : publier ses propres données tout en consommant des données publiées par quelqu'un d'autre. Le nombre de membres est illimité. Les composants de la plate-forme sont illustrés ci-dessous à la figure 3.

Le composant le plus important de la plate-forme est la passerelle. La passerelle encapsule toute la complexité de la sécurité pour les membres du système de partage de données. Les passerelles standardisent les processus de transfert de messages entre les membres du système de partage de données. Seuls l'expéditeur et le destinataire peuvent voir la structure et le contenu des messages.

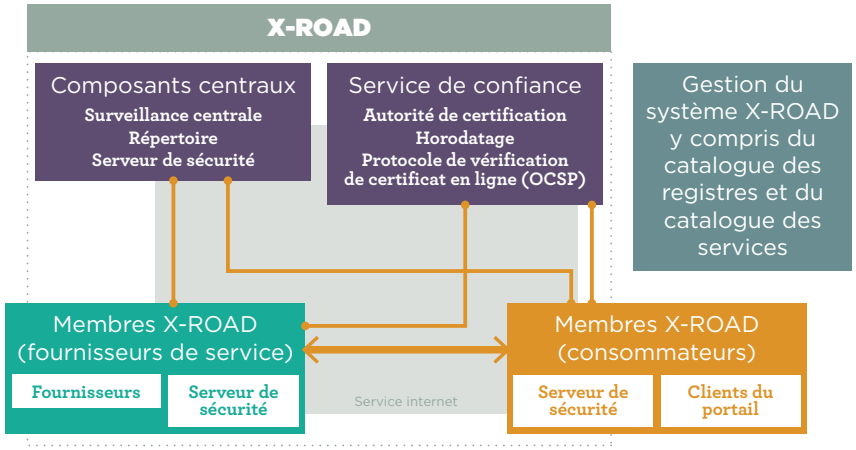


Figure 3: Composants d'infrastructure d'échange de données sécurisé

Le modèle implique seulement une quantité minimale de services centraux:

- **registre des systèmes et services d'information;**
- **identification et authentification par des tiers;**
- **journal des transactions;**
- **surveillance de la santé des services;**
- **fonctionnalité d'infrastructure à clé publique** (PKI).

Les composants centraux fournissent des informations aux serveurs proxy sur les participants à l'échange de données. Ces types de mécanismes permettent 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 faudrait surveiller le trafic pour détecter les intrusions, les modifications de données et d'autres types d'attaques.

La fourniture d'un échange de données sécurisé (c'est-à-dire signé, vérifié, chiffré et enregistré) via une plateforme d'échange de données nécessite plusieurs fonctions de gestion, notamment:

- **la gestion des services pour superviser toutes les communications d'identification,** d'authentification, d'autorisation, de transport de données, etc., y compris les autorisations d'accès, la révocation et l'audit;
- **l'enregistrement de service pour fournir** (sous réserve d'une autorisation appropriée) **l'accès aux services disponibles** par le biais d'une localisation préalable et d'une vérification de la fiabilité du service;
- **la journalisation des services pour garantir que tous les échanges de données sont consignés** pour des preuves futures et archivés si nécessaire.

Dans ce modèle d'échange de données sécurisé reposant sur le principe selon lequel les données sont échangées directement entre le fournisseur de données et le destinataire, sans intermédiaire central, il n'existe pas de point de défaillance unique. Cela signifie qu'il n'y a pas de risque unique de cyberattaque ou de 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.

RECOMMANDATION 62
L'administration doit utiliser un écosystème sécurisé d'échange de données pour échanger des données confidentielles.

4.4. Écosystème eID et PKI

L'identité numérique est la pierre angulaire du e-gouvernement. Tout simplement en possédant une identification électronique, les citoyens seront en mesure d'effectuer des transactions électroniques sécurisées et de tirer pleinement parti du gouvernement électronique et de la réduction des formalités administratives.

L'identification électronique (eID) est le processus consistant à utiliser les données d'identification d'une personne sous forme électronique, représentant uniquement une personne physique ou morale ou une personne physique représentant une personne morale.

Les services de confiance constituent un service électronique qui consiste en:

- **1. la création, la vérification et la validation de signatures électroniques,** de cachets électroniques ou d'horodatages électroniques, de services d'envoi électronique et de certificats liés à ces services;
- **2. la création, la vérification et la validation de certificats** pour l'authentification de sites web;
- **3. la préservation des signatures électroniques,** des sceaux ou des certificats liés à ces services.

La figure 4 décrit le modèle conceptuel d'infrastructure d'eID et de services de confiance. Une autorité d'enregistrement (RA) est chargée d'accepter les demandes de certificats numériques et d'authentifier l'entité

qui fait la demande. Une autorité de certification (CA) est une entité qui émet des certificats numériques. Un certificat numérique certifie la propriété d'une clé publique par le sujet nommé du certificat. Une autorité de validation (VA) est une entité qui fournit un service utilisé pour vérifier la validité d'un certificat numérique.

Lors de la construction de l'infrastructure pour les services d'identité et de confiance béninois, les composantes de l'écosystème doivent être dispersées autant que possible dans l'intérêt de la sécurité. La décentralisation garantit la transparence des processus et évite les risques de point de défaillance uniques, caractéristiques des systèmes monopolistiques centralisés. La construction des infrastructures pour les services d'identité et de confiance béninois doit se faire en impliquant des entités privées (banques, télécommunications, autorités de certification, etc.) et des institutions publiques (police, ministère de l'Intérieur, organisme de coordination informatique, organisme de mise en œuvre informatique, autorité de surveillance, etc.).

RECOMMANDATION 63

Il est recommandé de construire l'infrastructure de services d'identification et de confiance électroniques en partenariat avec des entités privées.

Les principales activités de l'infrastructure pour les services d'identité et de confiance béninois sont les suivantes :

- **activités de coordination visant à assurer l'interopérabilité de l'infrastructure** pour les services d'identité et de confiance béninois ;
- **préparation de la réglementation juridique de l'écosystème** pour les services d'identité et de confiance béninois ;
- **émettre des cartes d'identité et des identificateurs numériques** et s'assurer qu'ils disposent de certificats qualifiés délivrés par des fournisseurs de services de certification ;
- **s'assurer que les citoyens ont les moyens, via un service d'activation, de lier / activer leur eID** avec les certificats du fournisseur de service de certification qualifié ;
- **émettre des identifiants mobiles ;**
- **émission d'identifiants numériques** pour les citoyens et les non-citoyens résidents ;
- **émission de sceaux** ou cachets numériques ;
- **émission de certificats web ;**
- **supervision des fournisseurs de services** de confiance numériques ;
- **gestion du registre des services de confiance numériques ;**
- **fournir des services de certification ;**
- **fournir des services d'horodatage ;**
- **fournir les technologies et applications de signature numérique ;**
- **offrir des services de validation ;**
- **développer et administrer l'infrastructure** de signature numérique.

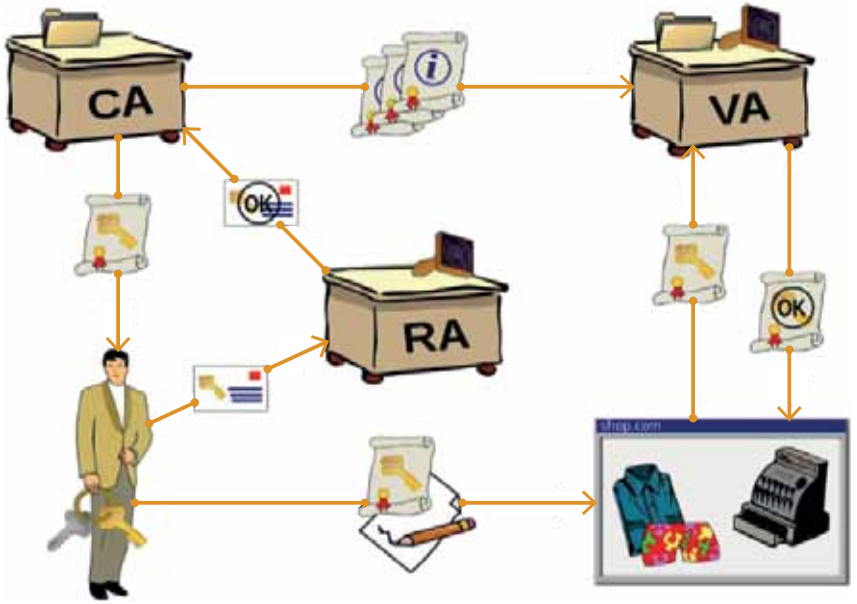


Figure 4 : Modèle conceptuel d'infrastructure d'eID et de services de confiance

4.5. Le catalogue des solutions d'interopérabilité

Les catalogues décrivent les services réutilisables et autres actifs afin d'améliorer leur capacité de recherche et leur utilisation. Ce composant permet aux éditeurs de documenter et de mettre à disposition des ressources susceptibles d'être réutilisées par d'autres. Il existe différents types de catalogues, par exemple des répertoires de services, des bibliothèques de composants logiciels, des portails de données ouverts, des registres de registres, des catalogues de métadonnées et des catalogues de normes.

Le catalogue de solutions d'interopérabilité (CatIS) est un instrument complémentaire pour la coordination des systèmes d'information d'état, un outil de développement et d'administration de systèmes inter-domaines et un système de support pour la maintenance des registres de base et des données de référence.

CatIS a pour objectif de garantir une gestion transparente, équilibrée et efficace des systèmes d'information du secteur public. CatIS 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 inclut des données sur des événements importants tels que : enregistrement d'institutions, intégration d'institutions au système sécurisé d'échange de données, etc.
- **Base de données de bases de données et de systèmes d'information :** ce composant fournit des métadonnées sur les registres gouvernementaux (DB) et les systèmes d'information (IS) : nom de DB ou IS ; propriétaire ; type de DB ou IS ; liste de services ; informations sur l'enregistrement et l'approbation ; architecture technique ; actes juridiques ; accords de niveau de service (SLA) ; paramètres de sécurité ; structure logique des données (objets de données, champs de données, paramètres de champs).
- **Entrepôt de services :** assure l'interopérabilité des systèmes d'information du secteur public et la réutilisation des ressources techniques, organisationnelles et sémantiques. L'entrepôt de services est un complément aux métadonnées conservées dans la base de données. Il inclut des spécifications pour tous les services web et une description détaillée des services gouvernementaux (y compris des descriptions de processus métier).
- **Entrepôt d'actifs sémantiques :** fournit des informations sur les composants réutilisables : actifs sémantiques, directives, etc.

CatIS 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. CatIS 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 utilisent ?**
- **Qui sont les responsables et les processeurs 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-elles exploitées et les données sont-elles traitées ?
- **Quels sont les composants réutilisables** assurant l'interopérabilité des systèmes d'information (actifs XML, classifications, dictionnaires et ontologies) ?

CatIS 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 plateforme d'échange sécurisé de donnée ;
- **Administration de composants réutilisables** (actifs XML, classifications, dictionnaires, ontologies).

CatIS fournit une assistance fiable et constitue un excellent outil pour les développeurs, les administrateurs et les utilisateurs du système d'information de l'État. CatIS offre des outils pour les activités coordonnées de plusieurs organismes. Les principales parties prenantes de CatIS sont illustrées à la figure 5.

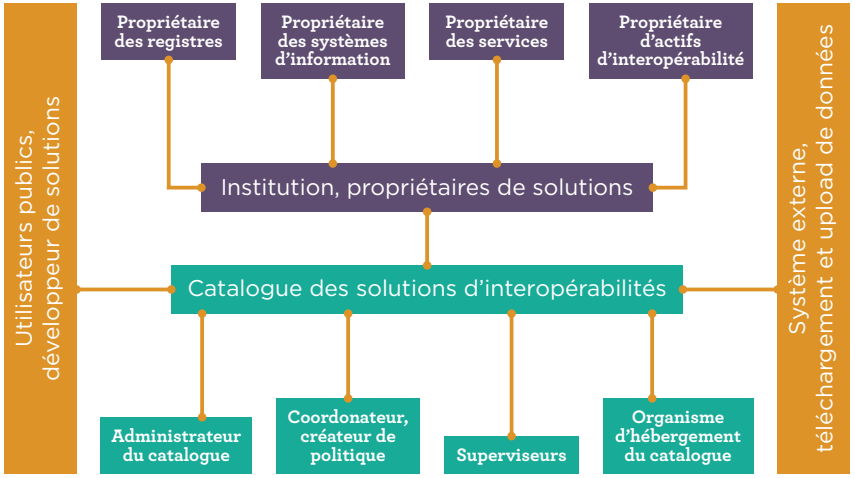


Figure 5 : Principaux acteurs de CatIS

RECOMMANDATION 64

Les administrations doivent enregistrer leurs systèmes d'information, leurs services et leurs actifs d'interopérabilité dans un catalogue de solutions d'interopérabilité.

Les parties prenantes créent ensemble 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 consommatrices sur leurs systèmes d'information, les propriétaires de services sur leurs services, les propriétaires d'actifs d'interopérabilité concernant leurs actifs. Les coordinateurs et les superviseurs utilisent le catalogue et y consignent leurs décisions.

4.6. Écosystème de données ouvertes (Open Data)

Si les gouvernements et les entreprises collectent un large éventail de données, ils ne les partagent pas toujours de manière facilement découvrable, utilisable ou compréhensible par le grand public.

Pour permettre une utilisation efficace des données, celles-ci doivent être soumises dans un format lisible par machine. Des règles explicites devraient être établies pour le recyclage des données, garantissant ainsi l'interopérabilité des systèmes et services d'information. Un écosystème de données ouvert doit être mise ne place pour prendre en charge le recyclage des données.

La mise en œuvre des données ouvertes contribuera à :

- **Transparence de la gouvernance :** l'implication des citoyens, leur autonomisation et l'ouverture de la recherche et des actifs culturels à leur utilisation est une obligation de tous les pays ;
- **Innovation :** les données ouvertes sont étroitement liées aux initiatives du gouvernement ouvert et aux nouvelles tendances technologiques, telles que les formats ouverts, les logiciels libres, les informations liées, les données volumineuses, le futur Internet et la co-création ;
- **Dynamiser l'économie :** l'ouverture des informations du secteur public permettra aux organisations du secteur privé et du tiers secteur de les combiner avec diverses données et de créer de nouveaux services aux entreprises à valeur ajoutée. Il n'est pas facile d'évaluer l'influence monétaire possible du recyclage des données sur la société, car elle est en grande partie indirecte.

Le Bénin a besoin de solutions aux problèmes suivants :

- **Développement et mise en œuvre d'une politique de données ouvertes** pour le Bénin ;
- **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 la base 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 ouvert pour le Bénin.

RECOMMANDATION 65

Les administrations doivent enregistrer leurs données ouvertes lisibles par machine sur un portail de données ouvertes.

4.7. Point de contact unique

Le portail des citoyens permet aux utilisateurs d'avoir accès à plusieurs systèmes d'information et portails sans avoir à se connecter plusieurs fois. Le portail permet l'accès à un certain nombre de services dématérialisés. L'accès au système est possible avec ou sans e-ID et, en fonction de la méthode d'accès, le nombre de services disponibles varie. Le portail des citoyens est le portail web officiel du gouvernement.

Le portail des citoyens offrira trois (03) sujets principaux : pour les citoyens, pour les entreprises et pour les visiteurs. Il est recommandé que le portail des citoyens élabore un environnement sécurisé personnel pour les citoyens auquel on accède par identification électronique. L'espace personnel peut contenir les sous-domaines suivants :

- **Zone de cycle de vie :** il contient des articles sur la façon de résoudre des problèmes importants ou fréquents (par exemple, la demande de prestations familiales) et des conseils sur les mesures à prendre dans certaines situations. Les services électroniques, les articles et les coordonnées du portail sont liés pour permettre aux utilisateurs de trouver facilement des informations relatives à certains sujets.
- **Zone de service électronique :** permet aux utilisateurs de consulter les données collectées par le gouvernement à leur sujet ;
- **Services de notification** (interruptions des livraisons d'électricité ou d'eau, expiration d'une période de validité, etc.) ;
- **Demandes :** permet aux personnes de remplir des formulaires puis de les transmettre aux institutions concernées ;

› **Zone de document sécurisé :** permet aux utilisateurs de signer et de transférer des documents.

Le sous-système de portail permet aux utilisateurs finaux d'accéder aux services électroniques de manière unifiée :

◆ PORTAIL DES CITOYENS : SERVICES POUR LE GRAND PUBLIC

L'utilisation du portail est pratique, sécurisée et permet de gagner du temps. Les citoyens et les étrangers peuvent trouver sur le portail des informations sur leurs droits et obligations en matière de communication avec les autorités publiques béninoises. Les informations détaillées contenues dans le portail peuvent être utilisées pour trouver des réponses à des problèmes potentiellement problématiques avant qu'ils ne surviennent. Les demandes 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 au même endroit, avec une réponse garantie. Tout le monde peut voir ses propres données. De plus, les citoyens peuvent voir qui a consulté leurs données personnelles dans des registres. Cela permet d'éviter un type d'abus lorsque de « curieux » agents de l'État examinent les données personnelles en dehors de leur champ d'action habituelle.

◆ PORTAIL DES AGENTS DE L'ÉTAT : SERVICES POUR LES AGENTS DE L'ÉTAT

Ce portail est un environnement sécurisé grâce auquel les utilisateurs ont facilement accès aux informations, services et coordonnées du secteur public. Les agents de l'État bénéficient de l'aide du portail pour ouvrir leurs propres ressources via un portail central.

◆ PORTAIL DES ENTREPRISES : SERVICES POUR LES UTILISATEURS PROFESSIONNELS

Ce 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 entrepreneurs des instructions pas à pas sur les mesures à prendre. Pour les opérateurs économiques, le portail représente un seul point de contact en ligne.

RECOMMANDATION 66

Un seul point de contact doit être mis à la disposition des utilisateurs afin de masquer la complexité administrative interne et de faciliter l'accès aux services publics, par exemple lorsque plusieurs organismes doivent collaborer pour fournir un service public.

5 ◆ GOUVERNANCE DES DONNÉES

5.1. Principes de gouvernance des données

Les données sont un élément fondamental de la mise en œuvre et de l'instauration du e-gouvernement. La gouvernance des données est la composante la plus importante de la gouvernance électronique. La gouvernance des données garantit que les données publiques sont à jour, sécurisées, cohérentes et standardisées. Pour faire confiance aux données, la confidentialité, l'intégrité et la disponibilité des données et des actifs doivent être assurées. La gouvernance des données définit le flux de données à travers les organisations.

La gouvernance des données est basée sur les principes suivants :

› **principe de légalité –** les données doivent être traitées dans une base de données appartenant au système d'information de l'État dans l'exercice de fonctions publiques liées aux obligations prescrites par un acte, une législation édictée sur la base d'un acte ou d'un accord international ;

› **principe d'unité –** les bases de données appartenant au système d'information de l'État doivent être compatibles entre elles et être capables d'interopérabilité, d'échange et de vérification des données ;

› **principe d'utilisation des données maîtresses –** lesdonnées doivent être recueillies à partir de sources aussi authentiques que possible et doivent être regroupées dans une base de données qui, en ce qui concerne les données correspondantes, doit être une source commune pour toutes les bases de données appartenant au système d'information de l'État tout en exerçant leurs fonctions imposées par la loi ;

› **principe de traçabilité –** toutes les demandes adressées à une base de données et les réponses fournies aux utilisateurs doivent être stockées (dans le cas de systèmes d'information interfacés avec la couche d'échange de données sécurisées des systèmes d'information, dans les journaux de sécurité des serveurs sécurisés). Il doit être possible d'établir et de restaurer des données dans une base de données et le fait de les traiter ;

- **principe d'utilisation des technologies de l'information à jour –** les possibilités offertes par les technologies de l'information à jour doivent être utilisées au maximum dans l'administration des bases de données appartenant au système d'information de l'État. Les données doivent être traitées numériquement ;
- **l'approche axée sur le service d'échange de données –** l'échange de données (utilisationcroisée) entre les différentes bases de données et les processeurs doit être effectué en fonction des services de données ;
- **principe d'optimalité technique et organisationnelle –** une base de données est établie et modifiée en tenant compte des principes d'administration du système d'information de l'État et sur la base des bonnes pratiques du domaine et du cadre d'interopérabilité ;
- **principe du secteur public axé sur les données –** reconnaît les données comme un atout, partie intégrante de l'élaboration des politiques, de la prestation des services, de la gestion organisationnelle et de l'innovation.

Des mesures organisationnelles, sémantiques et législatives (au besoin) doivent être mises en œuvre pour la gouvernance des données. La gouvernance des données est soutenue par les services d'infrastructure.

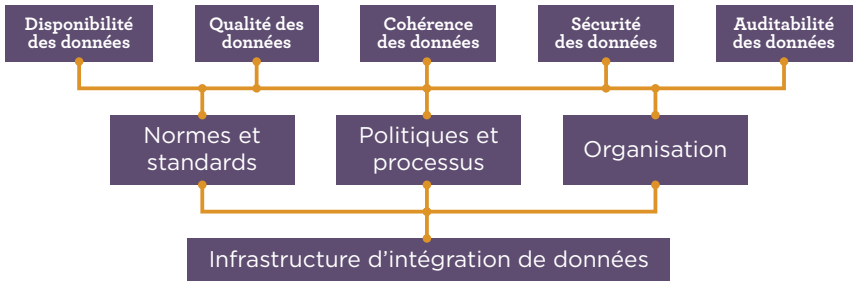


Figure 6 : Schéma conceptuel de la gouvernance des données

5.2. Niveau organisationnel

La gouvernance des données demande la création d'une structure dédiée basée sur le concept de « propriétaires » de données responsabilisés sur leurs zones d'expertise métier et IT. La responsabilité de la qualité des données doit être assurée par les métiers dans leur rôle de producteur ou de consommateur de la donnée. La structure de coordination assure le soutien des processus IT de la gouvernance par la mise en place de systèmes automatisés assurant la cohérence et l'intégrité des données. L'architecture SI et les solutions mises en place favorisent une gestion saine des données et sont le support d'une organisation pérenne de gestion de la qualité des données.

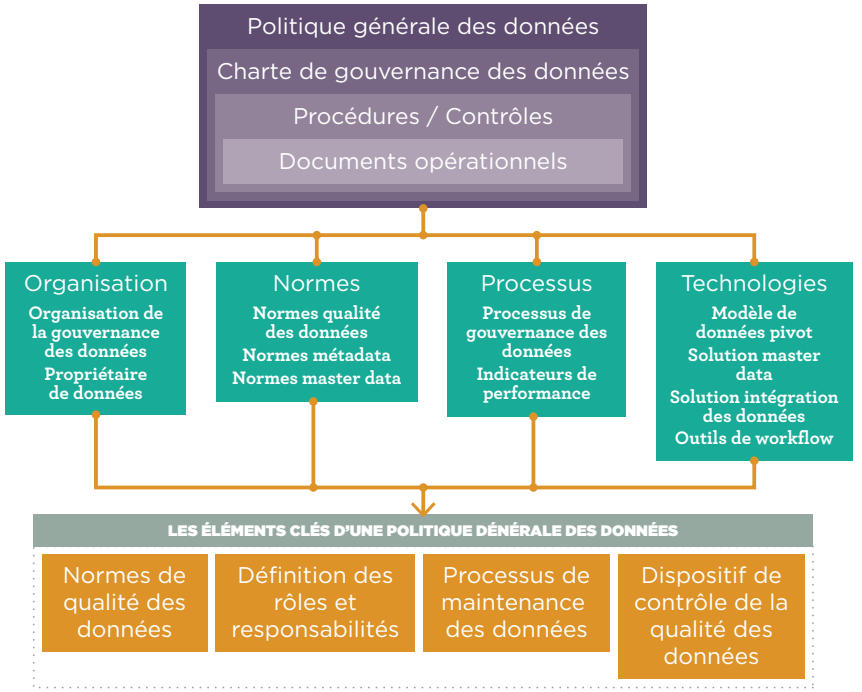


Figure 7 : Niveau organisationnel de la gouvernance des données

5.3. Niveau sémantique

Un dictionnaire de données reprenant le périmètre prioritaire des informations à échanger doit être élaboré, adopté, mis en application. Ce document doit décrire les libellés des données manipulées, leurs définitions, le cheminement pour les obtenir, l'administration qui en est responsable, leur emplacement dans les différentes bases de données.

RECOMMANDATION 67

Le Bénin doit mettre en place une gouvernance des données basée sur les principes de gouvernance de données.

6 ◆ CONCLUSION

Au cours des dernières décennies, les administrations béninoises ont investi dans les TIC pour moderniser leurs opérations internes, réduire leurs coûts et améliorer les services qu'elles offrent aux citoyens et aux entreprises. Malgré les progrès importants réalisés et les avantages déjà obtenus, les administrations se heurtent encore à des obstacles considérables en matière d'échange d'informations et de collaboration électronique. Ceux-ci incluent les barrières législatives, les processus commerciaux incompatibles et les modèles d'information, ainsi que 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 CdI favorise la communication électronique entre les administrations publiques béninoises 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 affaire de TIC, car elle a des implications multiples, allant du juridique à la technique. Le CdI identifie quatre (04) niveaux de défis d'interopérabilité (juridique, organisationnel, sémantique et technique) tout en soulignant le rôle essentiel de la gouvernance pour assurer la coordination des activités pertinentes à tous les niveaux et dans tous les secteurs de l'administration.

La structure de coordination DOIT avoir un mandat clair de la plus haute autorité. Il est important que la structure de coordination rende compte directement au Président de la République afin de s'assurer que les décisions et les progrès bénéficieront d'un soutien politique et de ressources de haut niveau.

Afin de garantir l'interopérabilité des systèmes d'information du secteur public, celui-ci développera et mettra en œuvre plusieurs composantes d'infrastructure communes. Les principaux composants ou catalyseurs de l'infrastructure béninoise d'administration en ligne sont :

- **l'écosystème sécurisé d'échange de données ;**
- **l'écosystème eID et services de confiance ;**
- **le catalogue des solutions d'interopérabilité ;**
- **l'Infrastructure Open Data ;**
- **le point de contact unique.**

Le CdI expose les principes et donne des recommandations concrètes pour la mise en place de ces services d'infrastructure.

1 FRAND : juste, raisonnable et non discriminatoire.

2 Cela favorise la concurrence dans la mesure où les fournisseurs travaillant sous différents modèles commerciaux peuvent se concurrencer pour proposer des produits, des technologies et des services fondés sur de telles spécifications.

4 http://tools.ietf.org/html/rfc4180

5 http://www.w3.org/wiki/HTML

6 http://www.evs.ee/tooted/evs-821-2009

7 www.w3.org/TR/REC-CSS2/

8 ISO 10918 (.jpg), http://www.jpeg.org/index.html.

9 RFC 1952

10 MPEG4 / ISO / IEC 14496

11 ISO / CEI 26300 : 2006, Format de document ouvert pour les applications Office (Open Document).

12 http://www.w3.org/TR/soap/

13 http://www.w3.org/TR/REC-png

14 http://www.w3.org/TR/SVG/

15 http://tools.ietf.org/html/rfc2306

16 http://www.w3.org/XML/

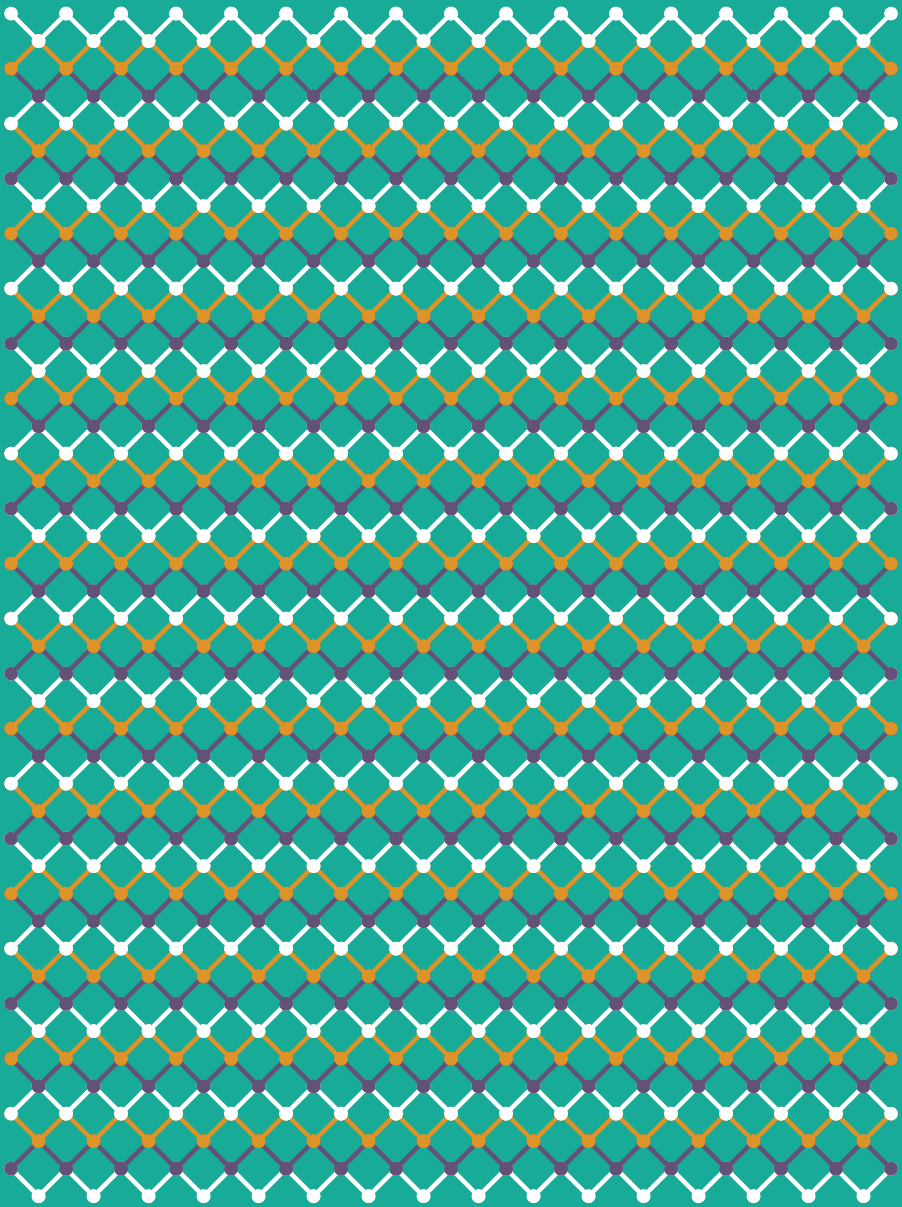
17 www.w3.org/TR/xsl/

18 http://www.w3.org/TR/WCAG20/

19 http://www.w3.org/TR/wsdl

www.xroad.bj

contact@xroad.bj



XROAD BJ