



---

**Ministère de l'Enseignement Supérieur, de la  
Recherche Scientifique et des Technologies  
de l'Information et de la Communication**

**Unité de Gestion du Projet WARCIP-Maurita-  
nie**

---

**ETUDE DE CADRAGE ET DE FAISABILITE  
POUR LA MISE EN PLACE D'UN  
SYSTEME DE DIGITALISATION DES  
SERVICES PUBLICS.**

---

*RAPPORT FINAL*

---

**NOVEMBRE 2020**    version V1.0

---



**Sofrecom**  
The Know-How Network



# Contacts

---

## Fawad Ali

**T** Direction Commerciale  
Area Sales Manager

**F** +33 (1) 57 36 33 64

**M** +33(6) 88 70 43 94

**E** [fawad.ali@sofrecom.com](mailto:fawad.ali@sofrecom.com)

24 avenue du Petit Parc  
94307 Vincennes - France

## Hicham Saoud

**T** Responsable du pôle eGouvernement

**F** +33 (1) 57 36 46 75

**M** +33(6) 78 17 15 53

**E** [hicham.saoud@sofrecom.com](mailto:hicham.saoud@sofrecom.com)

24 avenue du Petit Parc  
94307 Vincennes - France

## Revue et historique

Version	Auteur	Date	Modifications
V1.0	Equipe Sofrecom	18 Novembre 2020	Création

# Sommaire

---

Contacts .....	2
Liste des figures .....	5
Liste des tableaux .....	6
1. Rappel du contexte et des objectifs de l'étude .....	7
2. Rappel des conclusions de l'analyse de l'existant.....	9
2.1. Le développement des services en ligne comme axe prioritaire .....	11
3. Quelle vision pour développer les services digitaux ? .....	14
4. Quels services à digitaliser ? .....	17
4.1. Le catalogue des services à digitaliser à l'horizon de 2025 .....	17
4.2. Le premier lot des services à digitaliser .....	24
5. La solution technique proposée .....	26
5.1. Introduction.....	26
5.2. Axes directeurs de la solution technique.....	26
5.3. Architecture de la solution technique .....	27
5.4. Le socle nécessaire pour mettre en œuvre le premier lot des services.....	29
6. Le plan d'actions pour mettre en œuvre le premier lot des services digitaux .....	30
6.1. Les chantiers à lancer.....	31
6.1.1. Chantier 1 : Cadre juridique.....	31
6.1.2. Chantier 2 : Systèmes d'information.....	32
6.1.3. Chantier 3 : Démarches administratives .....	33
6.1.4. Chantier 4 : Cadre de gouvernance .....	34
6.1.5. Chantier 5 : Renforcement des capacités .....	35
6.1.6. Chantier 6 : Plateforme digitale.....	36
6.2. Le calendrier.....	38
6.3. Le budget estimatif .....	39
7. Annexes.....	45
7.1. Les scénarii de digitalisation des paiements publics en Mauritanie .....	45
7.2. Guide juridique et technique pour la création d'un service digital .....	58
7.2.1. Préambule.....	58
7.2.2. I- Questions préalables à la création d'un téléservice .....	64
7.2.3. II- Exigences pesant sur les données.....	70
7.2.4. III- Exigences pesant sur la Sécurisation des transactions électroniques.....	71

7.2.5.	IV- Cadre budgétaire de creation du service – Les marchés publics ou les PPP .....	80
7.2.6.	A- Glossaire .....	87
7.2.7.	C- Extraits de la Loi n° 2018-022 .....	88
7.2.8.	D- Elaboration des spécifications générales du service .....	90
7.3.	La gouvernance de l’urbanisation et la gestion des projets digitaux .....	96
7.3.1.	Rappel du cadre d’urbanisation des systèmes d’information de l’Etat.....	97
7.3.2.	La gouvernance du cadre d’urbanisation des systèmes de l’information de l’Etat.	102
7.3.3.	Quelques principes de gestion des projets SI .....	104
7.3.4.	Renforcement des capacités.....	108

## Liste des figures

---

Figure 1: Evolution de l'indice OSI de la Mauritanie .....	13
Figure 2 : Calendrier de la mise en œuvre du catalogue des services digitaux.....	24
Figure 3 Architecture globale de la solution .....	28
Figure 4 : Socle prioritaire de la plateforme digitale.....	29

## Liste des tableaux

---

Tableau 1 : Analyse des sites Web institutionnels.....	12
Tableau 2 : Evolution de l'indice OSI de la Mauritanie .....	13
Tableau 3: Liste des services à digitaliser.....	23
Tableau 4 : la liste des services prioritaires à digitaliser.....	25

# 1. Rappel du contexte et des objectifs de l'étude

---

La République Islamique de Mauritanie s'inscrit résolument dans une démarche de transformation digitale profonde de son administration visant l'augmentation de son efficacité, l'optimisation de ses dépenses, le désenclavement des territoires et l'amélioration de la qualité des services au profit des citoyens et des entreprises. Pour la Stratégie Nationale de Modernisation de l'Administration et des TICs, la transformation digitale se doit d'être rationnelle, optimale, efficace, efficiente et pérenne ; et ce :

- en élaborant les principes d'encadrement des projets, les modèles sur lesquels construire les systèmes d'information, les normes, les règles et les standards;
- en homogénéisant les différentes solutions organisationnelles et techniques de façon à veiller à la transversalité et à la compatibilité des systèmes intra gouvernementaux, mais aussi pour simplifier l'accès aux e-services pour les Citoyens et les Entreprises ;
- en positionnant les projets dans une perspective d'ensemble ;
- en garantissant que les objectifs poursuivis par le projet sont en phase avec la vision et les orientations stratégiques du pays ;
- en diminuant des coûts grâce à une organisation plus agile et plus optimale ainsi que la mise en commun et la réutilisation ; et
- en s'assurant que l'ensemble des systèmes d'information sont interopérables et sécurisés.

Dans ce contexte évolutif et dynamique, le gouvernement mauritanien souhaite réaliser une étude de cadrage et de faisabilité pour la mise en œuvre d'un système de digitalisation des services publics afin de doter la Mauritanie d'un cadre concret, ambitieux et réalisable pour le développement de l'administration électronique qui place le citoyen au centre de la préoccupation de l'administration en lui offrant des services de qualité et en promouvant l'accessibilité dans le but d'avoir une administration plus efficace, plus ouverte et plus transparente. Plus généralement, l'étude vise à favoriser l'émergence d'une offre de services électroniques complète et cohérente

Cette étude a pour objectifs, de faire :

1. Un état des lieux du cadre juridique et institutionnel de l'e-Gouvernement, des services numériques et des systèmes d'information en Mauritanie décrivant le gap dans ce domaine ;
2. Un état des lieux des infrastructures numériques et les contraintes techniques que doit prendre en considération toute solution de type e-Gouvernement pour qu'elle soit accessible à la majorité des citoyens et aux usagers de l'administration publique. Cet état des lieux ne doit pas couvrir seulement les aspects liés à la technologie mais aussi et surtout ceux liés à la Gouvernance de cette infrastructure. Les aspects liés à l'accès (afin de minimiser les conséquences de la future transformation induite par la digitalisation des services (exclusion, marginalisation, etc) doivent être adressés à ce niveau aussi. L'état des lieux couvre les infrastructures numériques nécessaires (réseau, serveurs, moyens d'accès par smartphone, par kiosques, zones d'accès...);
3. Une analyse des solutions techniques adéquates, ouvertes, optimales et à moindre coût pour la mise en place d'un système de digitalisation des services publics ;
4. Une analyse des scénarios économiques pour le financement de la mise en place de la plateforme e-Gouvernement de de digitalisation des services publics avec une analyse de leur durabilité ;
5. Une identification des moyens techniques d'interfaçage avec les systèmes de paiement nationaux pour permettre le paiement en ligne des services digitalisés et réaliser une revue des systèmes d'information principaux et des processus (back office) du

gouvernement afin de déterminer les éléments à mettre en place pour permettre leur dématérialisation. Il faut identifier, dans ce cadre, les moyens techniques permettant de rendre interopérables ces systèmes rendant possible les échanges de données ;

Une étude de la faisabilité technique, économique, financière, environnementale sociale, juridique et administrative afin d'évaluer l'intérêt potentiel du projet et ses impacts estimés.

## 2. Rappel des conclusions de l'analyse de l'existant

---

### **Des acquis à consolider et plusieurs freins à la digitalisation des services à lever**

L'étude de l'existant a permis de pointer les points forts et les faiblesses de l'écosystème e-Gouvernement de la Mauritanie.

En effet, la Mauritanie dispose d'un cadre juridique et institutionnel quasiment complet qui devrait supporter la digitalisation de l'administration publique. L'infrastructure télécoms du pays a connu de nombreux développements qui ont permis de satisfaire les exigences de connectivité des administrations publiques, mais l'effort de généralisation et de développement de l'accessibilité des citoyens et des entreprises recommandé par la stratégie de promotion de haut débit, est nécessaire pour développer les usages et assurer une meilleure inclusion numérique des usagers.

Les infrastructures d'hébergement des données recensées sont relativement modestes malgré les efforts déployés par la DGTIC à travers la mise à la disposition des ministères d'une infrastructure sécurisée pour héberger et exploiter leurs sites web et quelques applications et téléservices. Le projet de construction d'un data center gouvernemental respectant les normes internationales de sécurité permettrait à terme d'enrichir et de renforcer cette offre de services d'infrastructures numériques.

L'étude a par ailleurs montré que le système d'identité digitale et du registre national de la population est un véritable atout qui devrait permettre, à la fois aux administrations publiques de proposer des services numériques transactionnels requérant une forte authentification des usagers, mais également aux citoyens de disposer d'un moyen d'accès sécurisé aux services digitaux publics.

Si l'accès aux services digitaux est facilité par la mise en place de l'identité digitale, il est par ailleurs essentiel d'encourager leur adoption en permettant aux administrés de les régler à distance. Ainsi, la mise en place d'une plateforme de digitalisation des paiements permet d'assurer une dématérialisation de bout en bout des services publics.

Si l'offre et l'usage des services financiers digitaux restent limités, ceux-ci devraient être amenés à se développer avec le développement d'un cadre réglementaire propice. En effet, l'adoption prochaine d'une stratégie nationale d'inclusion financière et le projet de loi « portant sur les services et moyen de paiement » élaboré au mois de juin passé, fournissent de solides fondations stratégiques et réglementaires qui permettront aux transactions et services financiers digitaux de se développer.

En outre, la plateforme du GIMTEL peut faciliter le développement de ces services. C'est une solution technique robuste et sécurisée qui permettrait aux administrations publiques, moyennant la mise en œuvre des interfaces nécessaires, de proposer à leurs usagers de payer en ligne leurs démarches administratives.

Pour assurer une meilleure protection de ses services et infrastructures numériques, le gouvernement mauritanien a mis en œuvre plusieurs initiatives et projets. A cet effet, il convient de signaler que le cadre juridique de la cybersécurité complété récemment par une stratégie de cybersécurité permet au gouvernement de se doter d'un cadre assez riche pour instaurer la confiance numérique nécessaire pour développer les usages des services digitaux.

Les différents services de sécurité proposés aujourd'hui par la DGTIC pour sécuriser les infrastructures ainsi que les applications hébergées dans le data center national sont amenés à être

renforcés et enrichis avec la mise en œuvre du plan d'actions découlant de la stratégie nationale de cybersécurité.

Si ces nombreuses réalisations encourageantes témoignent de l'évolution positive de l'écosystème e-Gouvernement en Mauritanie, il convient de noter que l'étude a identifié plusieurs faiblesses qui entravent l'émergence d'une offre de services répondant aux attentes des usagers.

L'absence, jusqu'à récemment, d'un organe de coordination interministérielle dédié à l'e-Gouvernement était l'un des principaux obstacles du développement de la digitalisation des services publics. En effet, l'absence d'un organe interministériel pour assurer la gouvernance stratégique de l'e-Gouvernement entrave la mise en œuvre des initiatives et des synergies amorcées par la DGTIC. Cette situation a été échangée depuis l'adoption du décret N°2020-045/PM portant Création, missions et modalités d'organisation et de fonctionnement du Haut Conseil du Numérique (HCN), datant du 26 mars 2020.

La création du Haut Conseil du Numérique ainsi que son Comité Technique permet de répondre à cette faiblesse et d'apporter un dispositif de coordination concret et opérationnel représentant les principaux acteurs du paysage e-Gouvernement au niveau du pays.

Les ressources humaines, très peu nombreuses dans les directions TICs et systèmes d'information constituent une contrainte majeure qui appelle à un plan d'actions urgent pour renforcer les effectifs des ministères par des profils techniques ayant les compétences nécessaires pour concevoir, développer et exploiter les infrastructures et les services numériques.

L'élaboration d'un référentiel des services publics et des formulaires administratifs est un prérequis fondamental pour toute démarche de digitalisation. Malgré les efforts portés par la DGMA (Direction Générale de la Modernisation de l'Administration) en envisageant d'ouvrir un chantier interministériel portant sur la refonte et la simplification des procédures administratives, force est de constater qu'il existe aujourd'hui très peu de matière et de contenu à embarquer dans les infrastructures et les plateformes numériques.

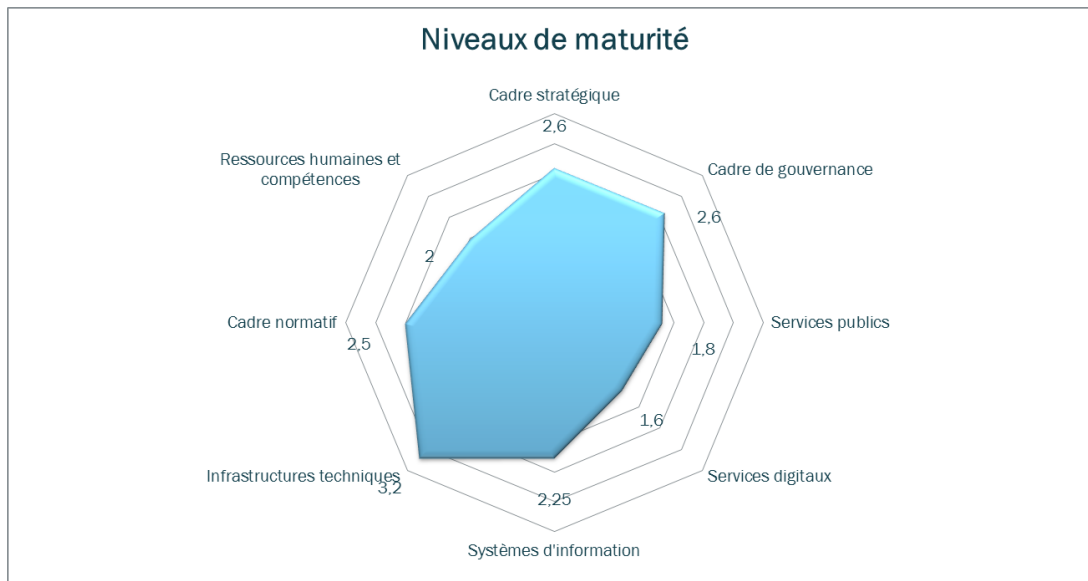
Par ailleurs, le niveau d'informatisation de l'administration mauritanienne est d'un niveau relativement faible. Si de nombreux systèmes d'information régaliens existent (budget, impôts, douanes, état civil, etc...), il y a lieu de noter qu'un grand nombre de métiers de l'administration sont manuels et ne sont pas supportés par l'informatique. La généralisation des systèmes d'information nécessiterait de renforcer les compétences techniques des agents publics mais également de définir une organisation et des dispositifs de gouvernance qui permettraient de mieux professionnaliser les fonctions des systèmes d'information à travers l'introduction des normes et des standards relatifs à l'architecture, l'urbanisation, la gestion des données, la gestion des risques et l'exploitation. L'élaboration du cadre général d'urbanisation des systèmes d'information (interopérabilité, sécurité, référentiel des données) va dans le sens de cette professionnalisation.

En somme, l'étude montre que le niveau de maturité de l'écosystème e-Gouvernement en Mauritanie est relativement moyen. La principale difficulté est d'opérationnaliser les différents cadres et stratégies définies. En effet, un gap important existe entre les pratiques du terrain et les nombreux cadres existants (textes juridiques, organigrammes et attributions, stratégies). En effet, malgré la forte volonté du Gouvernement Mauritanien de se doter des cadres nécessaires, force est de constater que les marges de manœuvre des acteurs publics sont très limitées au regard des moyens humains et financiers à leur disposition.

Le tableau ci-dessous présente le niveau de maturité de chaque composant. Cette maturité est mesurée sur une échelle de 1 à 5 :

- Niveau 1 : Très faible
- Niveau 2 : Faible

- Niveau 3 : Moyen
- Niveau 4 : Fort
- Niveau 5 : Très fort



## 2.1. Le développement des services en ligne comme axe prioritaire

L'e-Gouvernement a pour principal objectif d'améliorer l'accessibilité et la qualité des services publics afin de simplifier la vie des citoyens, des entreprises et des agents administratifs.

Cette simplification se concrétise à travers la mise en ligne des services informationnels et transactionnels à destination des usagers de l'administration publique.

La stratégie nationale de Modernisation de l'Administration et des TICs 2012-2016 a placé le développement des services en ligne comme un projet prioritaire pour mettre une administration électronique. L'orientation 47 « Développer les services en ligne » liste un certain nombre de services à destination des citoyens et des entreprises :

- Consultation du solde e-Service
- Développement des portails des Wilaya
- Suivi du courrier
- Service interactif des formalités administratives et de documents type
- Demande d'extrait du casier judiciaire
- Guichet en ligne pour l'accès aux services d'État civil et des titres sécurisés
- Consultation en ligne des Registres de Commerce (Pôle de services)
- Consultation de la situation fiscale et paiement des impôts en ligne
- Guichet unique de l'entreprise (Pôle de services)

L'étude d'évaluation de cette stratégie effectuée en 2017, estime le niveau de réalisation de cette orientation à 35%.

Un portail national des démarches administratives <http://www.servicepublic.gov.mr/> a été mis en place en 2008 par le MFPMa pour offrir aux usagers de l'administration publique mauritanienne

(particuliers, professionnels, diplomates, fonctionnaires et parlementaires) des informations pratiques et légales sur les différentes démarches administratives.

Ce portail qui a le mérite de présenter plus de 283 démarches administratives souffre de plusieurs lacunes et dysfonctionnements techniques et du problème de fiabilité et de mise à jour de son contenu.

Aujourd'hui tous les Ministères et la majorité des établissements publics disposent d'un site web. Une analyse de ces sites a permis de dégager quelques constats :

- La majorité des sites sont institutionnels (présentation du ministère, de son organisation, son cadre juridiques, ses attributions etc...).
- Très peu de sites offrent des informations pratiques sur les démarches administratives.
- Uniquement 28% des sites proposent des services transactionnels. La grande majorité de ces services sont très basiques.

**Tableau 1 : Analyse des sites Web institutionnels**

	Nombre de sites	% des sites
Nombre de sites institutionnels	41	87%
Nombre de sites interactifs (contact par mail)	25	53%
Nombre de sites fournissant des infos sur les démarches administratives	13	28%
Nombre de site proposant le téléchargement de formulaire	7	15%
Nombre de services transactionnels (20 services)	13	28%
Nombre de services intégrés	0	0%

Le croisement des résultats de cette analyse avec l'indicateur OSI (Online Services Index) de l'EGDI des Nations Unies confirme le niveau de maturité très bas des services en ligne en Mauritanie malgré les efforts déployés les 5 dernières années pour améliorer cet indice. Ce dernier a même baissé en 2020, cette régression s'explique par l'absence de services en ligne à destination des usagers mais également par les efforts déployés par d'autres pays qui ont réussi à améliorer leurs classements en déployant des services transactionnels.

Année	Rang	EGDI	Online Service Component
2014	174	0,1893	0,0472
2016	184	<b>0,1734</b>	0,0652

2018	183	0,2314	0,1597
2020	176	0,282	0,1

Figure 1: Evolution de l'indice OSI de la Mauritanie

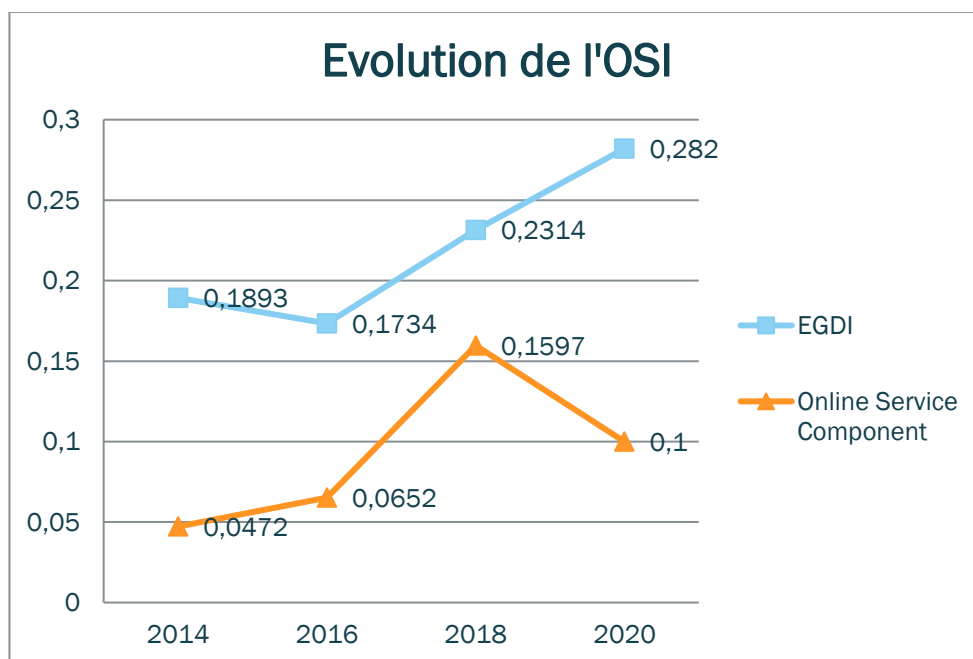


Tableau 2 : Evolution de l'indice OSI de la Mauritanie

### 3. Quelle vision pour développer les services digitaux ?

---

Le Gouvernement Mauritanien a placé la digitalisation des services publics comme un chantier stratégique et un levier de modernisation de l'administration Mauritanienne. Cette modernisation supportée par l'intégration et l'usage des Technologies de l'Information et de la Communication doit se concrétiser de façon réaliste, pragmatique, mesurable et progressive. La digitalisation des services a pour ambition de contribuer à la réalisation des objectifs suivants :

➤ **L'amélioration de l'information légale, administrative et économique**

La digital offre aujourd'hui, à travers les portails Internet, l'opportunité d'instaurer une administration communicante avec son environnement interne et externe.

L'administration numérique doit en premier lieu assurer la diffusion de tout type d'information publique et légale à destination des citoyens, entreprises et administrations.

La mobilisation des équipes du MESRSTIC pour finaliser la mise à niveau des sites institutionnels en 2020 et l'organisation et l'encadrement des équipes des ministères responsables de la mise à jour de ces sites sont nécessaires pour atteindre cet objectif.

**Au terme de 2022, 100% des informations administratives, légales, économiques seront disponibles en ligne**

**Information administrative** : il s'agit de l'information sur les démarches administratives.

**Information légale** : Il s'agit de fournir tous les textes de la législation mauritanienne : textes de lois, journal officiel, texte intégral des codes (civil, commerce, travail, etc.) ainsi que la jurisprudence et les actualités juridiques et législatives.

**Information économique** : il s'agit de toute information permettant de renforcer l'intelligence et la transparence économique pour aider les agents économiques (ménages et entreprises) à investir et à développer leurs activités économiques. Exemples : indicateurs socio-économiques, statistiques sur la consommation, prix des matières premières, prix de l'énergie, emploi et chômage, les aides et les subventions de l'Etat, etc...

Pour arriver à atteindre cette cible, les leviers suivants sont nécessaires :

- Cartographie et modélisation des démarches administratives
- Mise en œuvre d'un référentiel des formulaires administratifs
- Numérisation des textes législatifs
- Mise en œuvre d'un gisement des données économiques
- Mise en œuvre de la charte graphique institutionnelle
- Généralisation des sites web pour publier les informations publiques
- Définition et mise œuvre d'une organisation et d'une gouvernance du cycle de vie des données publiques : création, modification, stockage et suppression.

➤ **La transparence administrative**

La modernisation administrative par les TIC supporte la transparence publique porteuse de valeurs de bonne gouvernance. Dans ce sens, le Gouvernement Mauritanien considère la digitalisation comme un levier pour renforcer le processus de transparence dans la vie publique et économique.

### **Au terme de 2023 : Toutes les données publiques seront disponibles en ligne**

Pour arriver à atteindre cette cible, les leviers suivants sont nécessaires :

- Définition d'une stratégie d'ouverture des données publiques répondant à ces questions : quels sont les objectifs et les bénéfices recherchés ? quelles sont les données à ouvrir ? Comment exposer ces données ? quels sont les contrôles d'utilisation et de réutilisation à mettre en place ?
- Mise en œuvre d'une plateforme technique Open Data
- Inventaire des données publiques et identification des éventuelles contraintes à l'ouverture (contraintes juridiques et administratives)
- Définition et préparation des données prioritaires (jeux de données, choix des formats, documentation)
- Diffusion et valorisation des données
- Mise en œuvre d'une organisation et des processus de mise à jour, d'animation et de valorisation de la réutilisation des données.

#### ➤ **Le développement de la proximité et de l'accessibilité des services publics**

L'accessibilité des services publics aux Mauritaniens est l'un des enjeux majeurs de la digitalisation. Le développement du numérique permettra de faciliter l'accès des citoyens et des entreprises aux services publics. Un catalogue de services digitaux sera présenté dans le présent rapport. L'objectif est de créer 110 services en ligne avant la fin de 2025

Pour arriver à atteindre cette cible, les leviers suivants sont nécessaires :

- 1) Mise en place, en 2021, d'une plateforme technique permettant le développement aisé des services en offrant un portail fédérateur qui redirige vers les différents services publics digitalisés, une couche Gateway d'API d'interfaces standardisée avec les fournisseurs de service externes (prestataire de service de paiements ...), un module commun de gestion des identités et des accès (IAM), une panoplie de services Core mis à disposition à travers des API, un moteur de Règles et de Workflows (générateur de Rules & Workflow), un modèle de gestion d'un référentiel de données unifié et moteur de BI avec outils de visualisation de données .....
- 2) Déploiement dès 2021, au moins de 3 familles de services parmi celles identifiées durant l'étude : « Etat civil et papiers d'identité ; Casier judiciaire ; Inscription aux concours ; Permis de construire ; Création d'entreprise ; Plateforme RDV ; Paiements ; Demande de visa ; Espace étudiant ; Espace Agent »
- 3) Enfin, chaque ministère s'engagera à mettre en œuvre au moins un service digital par an à partir de 2021.

### **Au terme de 2025 : 110 services digitaux seront créés par les Ministères**

#### ➤ **L'amélioration de l'environnement des affaires**

Le développement du digital représente un levier d'amélioration de la compétitivité économique de la nation. L'informatisation des PME, la mise en ligne des services destinés aux entreprises, le

renforcement des capacités TIC des employés sont des enjeux majeurs pour améliorer la productivité et par conséquent la compétitivité de l'entreprise Mauritanienne.

Pour améliorer son environnement des affaires, le gouvernement Mauritanien se doit d'envisager le lancement d'un vaste programme de digitalisation prenant en compte tous les services liés aux indicateurs Doing Business (création d'entreprise, raccordement à l'électricité, obtention du permis de construire, enregistrement des contrats, etc...)

**Au terme de 2025 : 100% des démarches administratives supportant les indicateurs Doing Business seront digitalisés.**

➤ **L'amélioration de l'efficacité et de l'efficience publiques**

Dans un contexte de crise économique internationale, les gouvernements doivent faire aussi bien avec moins de moyens financiers. Les TIC sont des outils pour aider le Gouvernement Mauritanien à optimiser son fonctionnement interne.

La digitalisation des services publics doit être considérée comme une opportunité pour simplifier les processus administratifs et automatiser les échanges inter-administrations.

La digitalisation des services publics doit s'inscrire dans ce cadre, une analyse systématique de la valeur publique au sens large (économique, politique, démocratique) doit être menée préalablement à chaque projet pour évaluer le retour sur l'investissement et les effets de la digitalisation.

**Au terme de 2025 : 20% des échanges des documents entre les administrations seront dématérialisés.**

➤ **Le rayonnement international et le Leadership Régional**

Le développement du digital au delà des impacts socio-économiques, participera au rayonnement de la Mauritanie sur la scène régionale et internationale.

En 2020, La Mauritanie est classée 176 sur 193 (L'indice de développement eGouv est évalué à 0.2820). Le Gouvernement affiche l'ambition d'améliorer sensiblement cette position dans les prochaines années.

**Au terme de 2022 : La Mauritanie sera parmi les 140 premiers pays de l'eGouv au niveau mondial**

**Au terme de 2024 : La Mauritanie sera parmi les 120 premiers pays de l'eGouv au niveau mondial**

## 4. Quels services à digitaliser ?

### 4.1. Le catalogue des services à digitaliser à l'horizon de 2025

En concertation avec le Comité de Pilotage et les points focaux de l'étude, une liste des services publics à digitaliser a été arrêtée. Cette liste intègre des services destinés aux citoyens (G2C), aux entreprises (G2B) et aux agents publics (G2E).

Domaine	Services	Citoyen	Entreprise	Agent
Etat civil - Citoyenneté	Demande d'acte de naissance	X		
	Demande d'acte de mariage	X		
	Demande d'acte de décès	X		
	Demande de rectification d'un acte d'état civil	X		
	Pré-demande de carte d'identité	X		
	Pré-demande de passeport	X		
	Achat en ligne du timbre fiscal - Passeport	X		
	Suivez votre demande de carte d'identité	X		
	Suivez votre demande de passeport	X		
	Extrait d'acte de naissance	X		
Education	Inscription aux concours nationaux	X		X
	Accès en ligne à l'espace d'orientation universitaire	X		
	Inscription universitaire en ligne	X		
	Demande, consultation et suivi des bourses	X		
	Demande, consultation et suivi de logement	X		
	Demande d'autorisation d'enseigner	X		X
	Demande d'équivalence d'un diplôme	X		

	Demande d'attestation d'Équivalence de Diplôme	X		
<b>SOCIAL - SANTÉ</b>	Plateforme de prévention	X		
	Réservation en ligne de vaccination	X		
	Annuaire des professionnels de santé	X	X	X
	Calendrier vaccinal	X		
	Demande d'affiliation à la CNAM	X		
	Faire le suivi du recouvrement des frais de traitement par les assurés sociaux	X		X
	Prise de RDV à l'hôpital	X		
	Demande de certificat médical	X		X
	Carnet de vaccination	X		
<b>TRAVAIL</b>	Consultation des offres d'emploi mises en ligne	X		
	Mise en ligne de CV pour les chercheurs d'emploi	X		
	Dépôt en ligne d'offres d'emploi par les employeurs et consultation de la base des candidats		X	
	Demande d'inscription à l'agence d'emploi	X		
	Inscription aux concours	X		X
	Délivrance de la carte de demandeur d'emploi	X		
	Délivrance de la carte de travail	X		
	Demande d'inscription à une formation professionnelle	X	X	X
<b>Transport</b>	Demande de candidature aux examens du permis de conduire national	X		
	Consultation des délais des examens de permis de conduite	X		
	Examen blanc du permis de conduire	X		
	Demande de duplicata de permis de conduire national	X		
	Horaires des vols	X	X	X
	Réservation en ligne de billets de vols	X	X	X
	Suivi des bagages retardés	X	X	X

	Demande de carte grise	X	X	
	Demande de duplicata de carte grise de véhicule	X	X	
	Demande d'Immatriculation de véhicule	X	X	
	Demande de transport de véhicule	X	X	
	Demande de carte grise internationale de véhicule automobile	X	X	
	Demande de permis de conduire international	X		
	Consultation et paiement des infractions routières	X	X	
<b>Impôts &amp; taxes</b>	Déclaration des impôts	X	X	
	Paiement des impôts et taxes	X	X	
	Achat de timbre fiscal	X	X	
	Demande de situation fiscale	X	X	
	Demande d'attestation de régularité	X	X	
	Demande d'attestation de non-imposition	X	X	
	Déclaration et paiement de la TVA		X	
	Demande d'attestation de quitus fiscal	X	X	
<b>Trésor</b>	Attestations de régularité		X	
	Attestation de précompte		X	
	Main levée		X	
<b>Paiements en ligne</b>	Paiement en ligne des amendes issues du contrôle routier	X	X	
<b>Finances</b>	Demande de titre foncier	X	X	
	Espace de téléchargement de formulaires douaniers	X	X	
	Démarches douanières en ligne	X	X	
	Enregistrement des contrats	X	X	
<b>Habitat</b>	Ajout et modification de composants de bâtiment	X	X	
	Permis de rénovation de bâtiment	X	X	

	Demande de permis de construction	X	X	
	Renouvellement du permis de construction	X	X	
	Demande de permis d'occuper	X	X	
<b>Justice</b>	Accès des plaideurs au guichet de suivi des plaintes, des procès-verbaux et des affaires auprès des tribunaux	X	X	
	Demande de casier judiciaire	X		
	Suivi des affaires judiciaires	X	X	
	Demande de régularisation de l'état civil	X		
	Accès des avocats au guichet de suivi des plaintes, des procès-verbaux et des affaires auprès des tribunaux	X	X	
<b>Agriculture &amp; Pêche &amp; Elevage</b>	Place de marchés des produits agricoles	X	X	
	Demande de subventions	X	X	
	Demande d'accès aux intrants agricoles (semences, engrais)	X	X	
	Demande d'équipements d'irrigation	X	X	
	Demande d'accès aux équipements agricoles	X	X	
	Demande d'autorisation d'importation des animaux, des produits animaux et des produits d'origine animale		X	
	Demande d'établissement d'un certificat à l'exportation		X	
	Demande d'établissement d'un certificat de salubrité		X	
	Demande d'une concession de pêche ou d'aquaculture		X	
	Demande de certificat d'accréditation		X	
	Demande de licence pour commerçant / maireur		X	
	Demande d'un permis de pêche	X	X	

	Demande de licence d'exploitation des ressources halieutiques		X	
	Demande de subventions	X	X	
<b>Investissement et environnement des affaires</b>	Création d'entreprise		X	
	Déclaration d'embauche		X	
	Raccordement à l'électricité	X	X	
	Enregistrement des contrats		X	
	Permis de construire	X	X	
	Déclaration et paiement des impôts	X	X	
	Déclaration et paiement de la TVA		X	
	Paiement des cotisations sociales		X	
	Demande d'autorisation d'exercice de métiers réglementés (avocat, notaires, expert-comptable...)		X	
	Autorisation de l'exercice de l'activité artisanale		X	
	Plateforme de marchés publics		X	
	Demande d'autorisation d'import/export		X	
	Certificat d'Origine des marchandises		X	
	Déclaration Préalable d'Importation		X	
	Autorisation d'Exercer le Commerce		X	
	<b>Agent</b>	Demande de congés		
Demande de promotion				X
Demande d'autorisation d'absence				X
Inscription aux concours				X
Demande de formation				X
Demande de retraite + anticipée				X
Demande d'attestation d'employeur				X
Demande de mise en disponibilité				X

	Demande de mutation			X
	Demande d'attestation de service effectué			X
<b>Tourisme</b>	Demande de visa de validation de la licence d'agence de voyages et de tourisme		X	
	Demande de la carte professionnelle de guide de tourisme	X	X	
	Demande d'autorisation d'exploiter des restaurants de tourisme		X	
	Demande de licence des agences de voyage et de tourisme		X	
	Demande d'autorisation d'exploiter des établissements touristiques d'hébergements.		X	
	Demande de renouvellement de la carte professionnelle de guide de tourisme	X	X	
<b>e-Démocratie</b>	Plateforme de eParticipation	X	X	X
<b>Pèlerinage</b>	Inscription en ligne au Hajj	X		
<b>Services aux Mauritaniens à l'étranger</b>	e-Rendez-vous : Service en ligne de prise de rendez-vous pour se rendre aux ambassades ou consulats	X		
	Inscription consulaire en ligne permettant aux Mauritaniens expatriés de consulter et modifier leurs données personnelles, leur situation électorale et commander des actes d'état civil.	X		

**Tableau 3: Liste des services à digitaliser**

## 4.2. Le premier lot des services à digitaliser

La mise en œuvre de la digitalisation des services prévoit de nombreux projets qu'il est nécessaire d'organiser et d'ordonnancer les uns par rapport aux autres dans le cadre d'une approche pragmatique et réaliste. Cette approche doit :

Amorcer la digitalisation des services prioritaires et démarrer les premières instanciations de la plateforme technique à mettre au point.

En parallèle à ce premier lot, les chantiers identifiés lors la phase de l'analyse de l'existant devraient être lancés pour préparer le plaiement progressif et accéléré de la digitalisation des services à l'horizon de 2025. Il est important d'adresser les faiblesses majeures identifiées qui risquent d'entraver le développement de la digitalisation, notamment :

- L'opérationnalisation rapide des instances de gouvernance (HCN)
- Le lancement du chantier de cartographie et de simplification des démarches administratives
- L'élaboration du référentiel des formulaires administratifs
- ...

Ensuite, la digitalisation de l'ensemble des services devraient être étalés à l'horizon de 2025. Un cadre précis définissant les indicateurs et les objectifs de digitalisation doit être proposé pour piloter l'avancement de la digitalisation.

- 2021 : 12 services
- 2022 : 23 services
- 2023 : 25 services
- 2024 : 25 services
- 2025 : 30 services

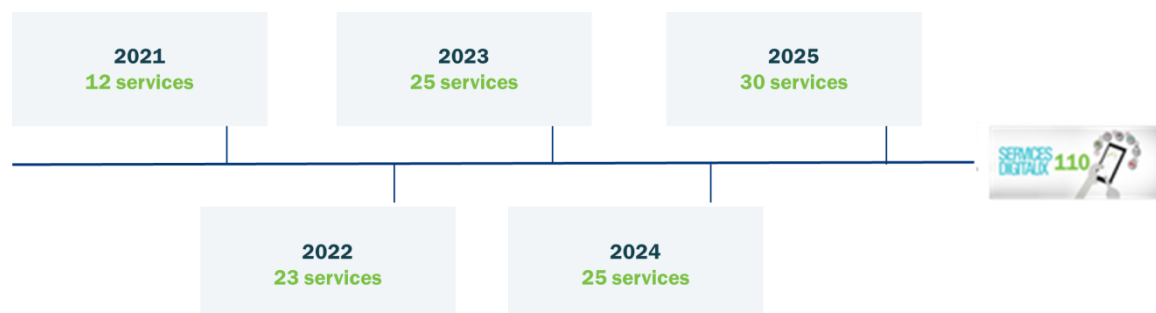


Figure 2 : Calendrier de la mise en œuvre du catalogue des services digitaux

En concertation avec le Comité de Pilotage de l'étude, nous proposons un premier lot de  $n$  services à identifier parmi ceux des 11 familles de services à digitaliser ci-dessous. Ce bouquet regroupe un ensemble de services prioritaires qui s'adressent à tous les usagers (Citoyens, Entreprises et Agents).

	Démarches	Usagers			Ministère/Entité	Nombre de services
		Ci- toyen	Entre- prise	Agent		
1	État civil et papiers d'identité (10 services)	X			MIDEC/ ANRPTS	3
2	Casier judiciaire	X			MJ	1
3	inscription aux concours	X		X	MFPTMA & ME-SRSTIC	1
4	Permis de construire	X	X		MHUAT	1
5	Démarche de la CNSS	X	X		CNSS	4
6	Plateforme RDV	X	X	X	MESRSTIC	1
7	Paiement	X	X	X	MESRSTIC, GIMTEL, MF	1
8	demande de visa	X	X		MIDEC / ANRPTS	1
9	Espace étudiant	X			MESRSTIC	5
10	Espace Agent (			X	MFPTMA	5
11	Demande des autorisations / agréments		X		Guichet Unique	1

Tableau 4 : la liste des services prioritaires à digitaliser

## 5. La solution technique proposée

---

### 5.1. Introduction

La Solution technique du système de digitalisation des services publics permet de fournir un cadre global de la solution à mettre en place pour répondre à l'ensemble des enjeux de cette transformation. Il tient compte des exigences générales suivantes :

- **Intégrité** : afin d'assurer que les données sensibles et protégées ne soient pas modifiées indument, des composants assurant l'intégrité de la données de bout en bout sont intégrés dans la solution.
- **Couplage lâche** : une faible adhérence entre les différentes briques qui composent solution technique. Plusieurs composants permettent d'avoir une adhérence faible avec ses interfaces externes (interface avec les applications des partenaires métiers et partenaire de service, ..) et internes (ses propres services, ses propres composants d'intégration, de base de données, ...).
- **Simplicité** : Une architecture simple et interopérable permet de mettre en place des composants et des briques dans un écosystème facilement extensible et stable dans la durée.
- **Évolutivité** : (ou Scalabilité) l'évolutivité de la solution permet d'absorber les nouvelles demandes fonctionnelles ainsi que les contraintes de capacité de traitement et de volumétrie de données.
- **Sécurité** : Sécuriser l'accès aux différents fronts ends, Backends et données sensibles.

La proposition de solution tient également compte des exigences de la solution cible en termes de :

- **Prise en compte de l'existant (Le Legacy)** : elle tient compte de l'analyse faite durant la phase de « Étude de l'existant (Phase 2 du projet) ».
- **Respect des exigences de sécurités référencées** dans le Cadre général de la sécurité.
- **Respect des exigences et des recommandations du Cadre Général d'Interopérabilité.**
- **Respect des exigences et des recommandations du Cadre Général d'Urbanisation des systèmes d'Information de l'État.**
- **Décomposition en briques fonctionnelles et techniques** permettant de lotir la mise en œuvre en fonction des besoins et des contraintes budgétaires.
- **Le projet de mise en place d'un Cloud Gouvernemental** qui hébergera les applications qui y sont éligibles.

### 5.2. Axes directeurs de la solution technique

Afin de décrire la solution technique à mettre en place, nous commençons par définir les axes directeurs de la plateforme :

- **Un portail fédérateur** : redirection vers les différents sites des Ministères et des organismes publics proposant des services publics digitalisés aux usagers.
- **Une couche Gateway d'API** : fournir aux différents Ministères et organismes publics des interfaces uniques et standardisées : intégration unique avec les fournisseurs de services externes (prestataires de services de paiements par exemple).
- **Une gestion des identités et des accès (IAM).**
- **Une panoplie de services Core** mis à la disposition des autres partenaires à travers des APIs.
- **Un moteur de Règles et de Workflows** : Générateur de règles & Workflow.

- Un référentiel unifié de données et un moteur de BI fournissant des outils de visualisation de données en mode PAAS ainsi qu'un entrepôt de données et un ETL pour le chargement de données.
- Un hébergement dans un Cloud privé : gestion des parties Hardware, exploitation hardware en mode (IAAS) et possibilité de proposer du SAAS.

L'ensemble de ces axes constituent la feuille de route de la mise en place de la solution technique

### 5.3. Architecture de la solution technique

La solution technique est composée de Cinq grandes briques permettant :

- Une décomposition simple en modules fonctionnels et techniques avec le minimum de couplage : Cette propriété va permettre de faciliter l'implémentions de ce chantier en permettant de le décomposer en plusieurs programmes et projets à étaler dans le temps.
- Un découplage entre les différentes partie Front-end et Backend (indépendance technique et fonctionnelle).
- Une instanciation globale avec des référentiels communs de données quand c'est possible.
- L'évolutivité (Scalabilité) d'une façon simple sans avoir à transformer toute l'architecture pour supporter la montée en charge de la capacité de traitement des systèmes d'information à mettre en place.
- La séparation fonctionnelle des systèmes :
  - Regrouper les systèmes d'opérations qui vont supporter les fonctions de Build (Construction) et de Run (Exploitation) du système d'information.
  - Regrouper les systèmes d'analytiques qui vont alimenter les processus de Think (Cadrage et étude) du système d'information.
  - Regrouper les systèmes d'interactions (Front end) dans un ensemble de fonctions d'interaction avec le système d'information.

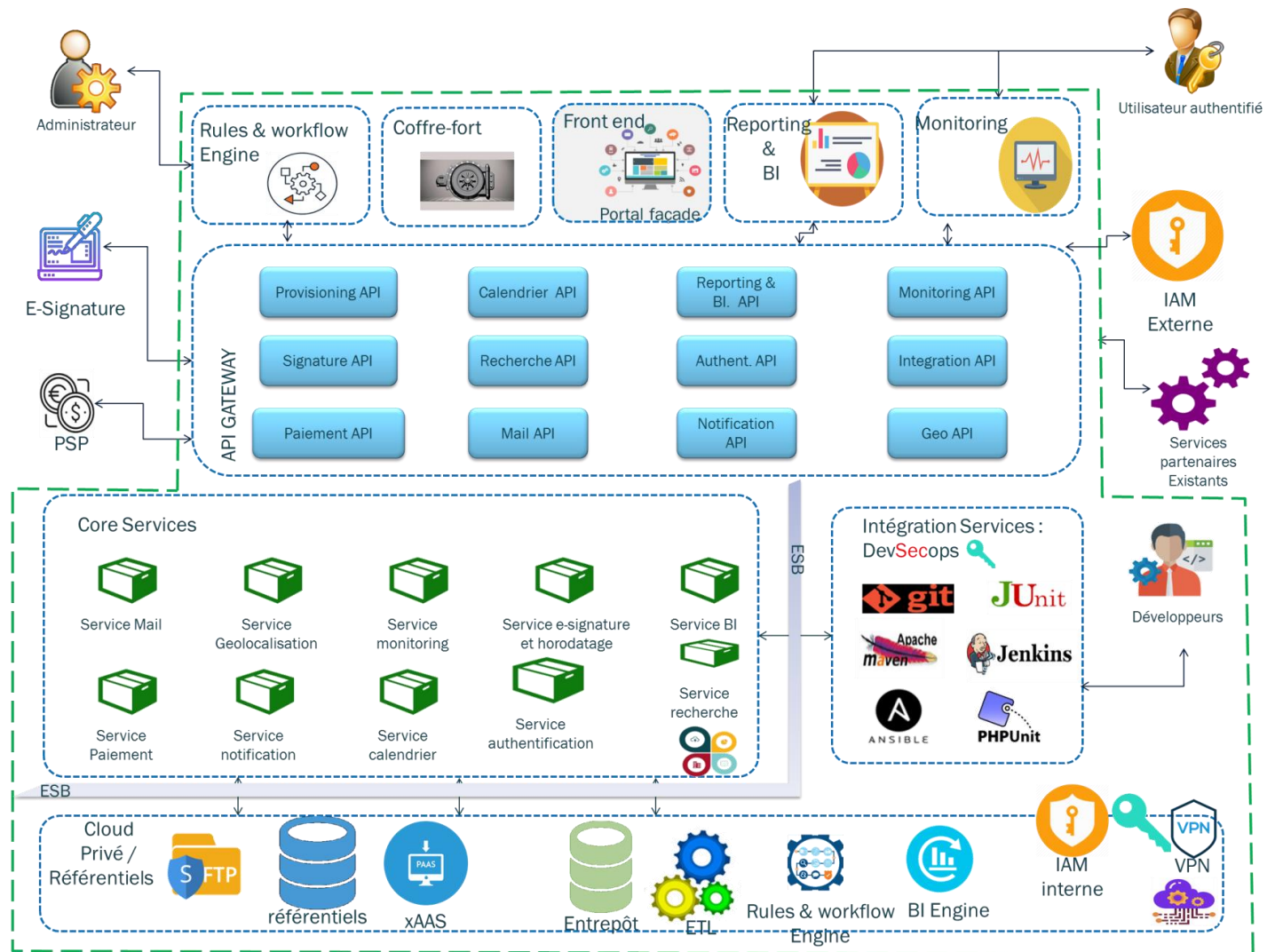


Figure 3 Architecture globale de la solution

## 5.4. Le socle nécessaire pour mettre en œuvre le premier lot des services.

Pour mettre en œuvre le premier lot des services digitaux, nous proposons d'acquérir un premier socle de la plateforme digitale incluant les briques suivantes :

- Plateforme portail et moteur de workflow
- Plateforme de Business Intelligence
- Solution de supervision
- Plateforme d'API
- Plateforme de gestion d'identité (IAM)
- Coffre-fort électronique

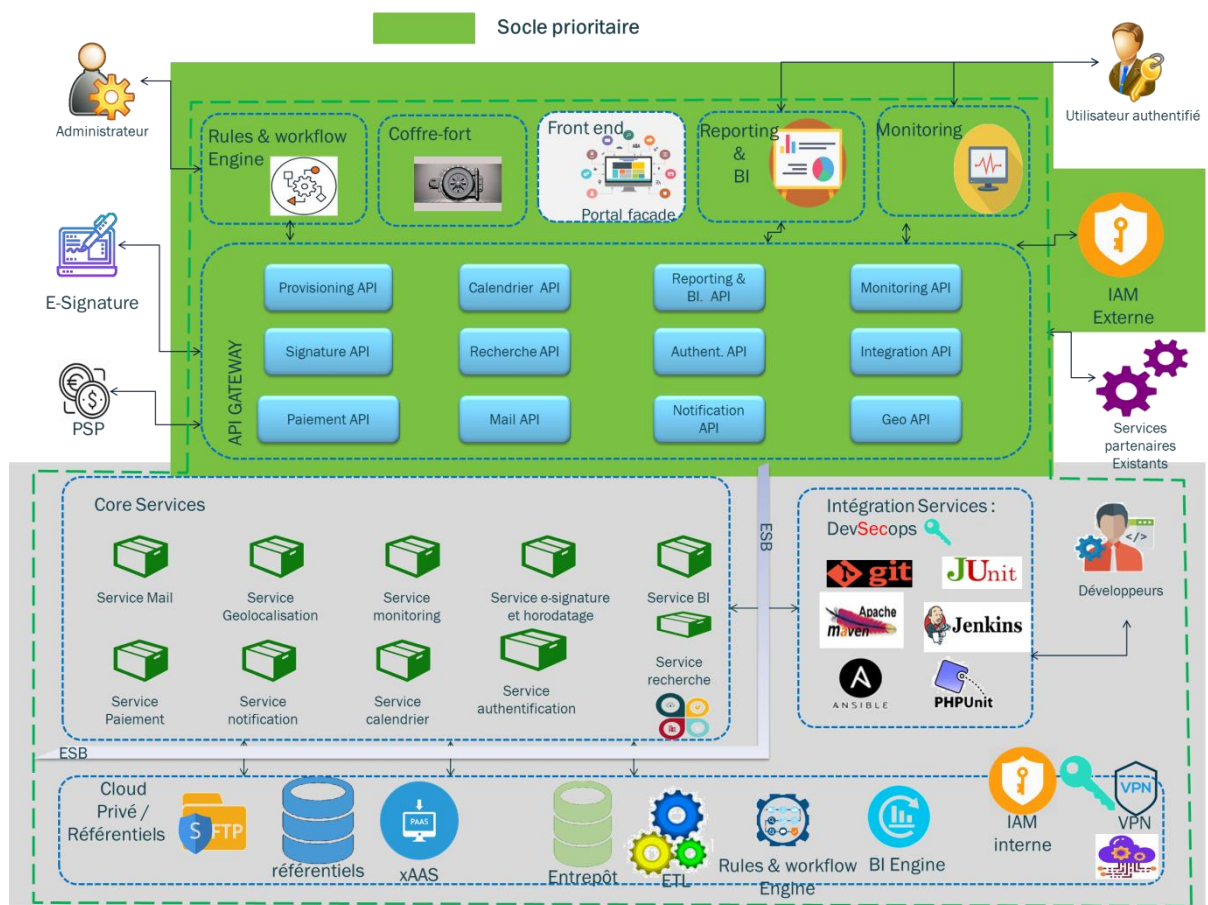


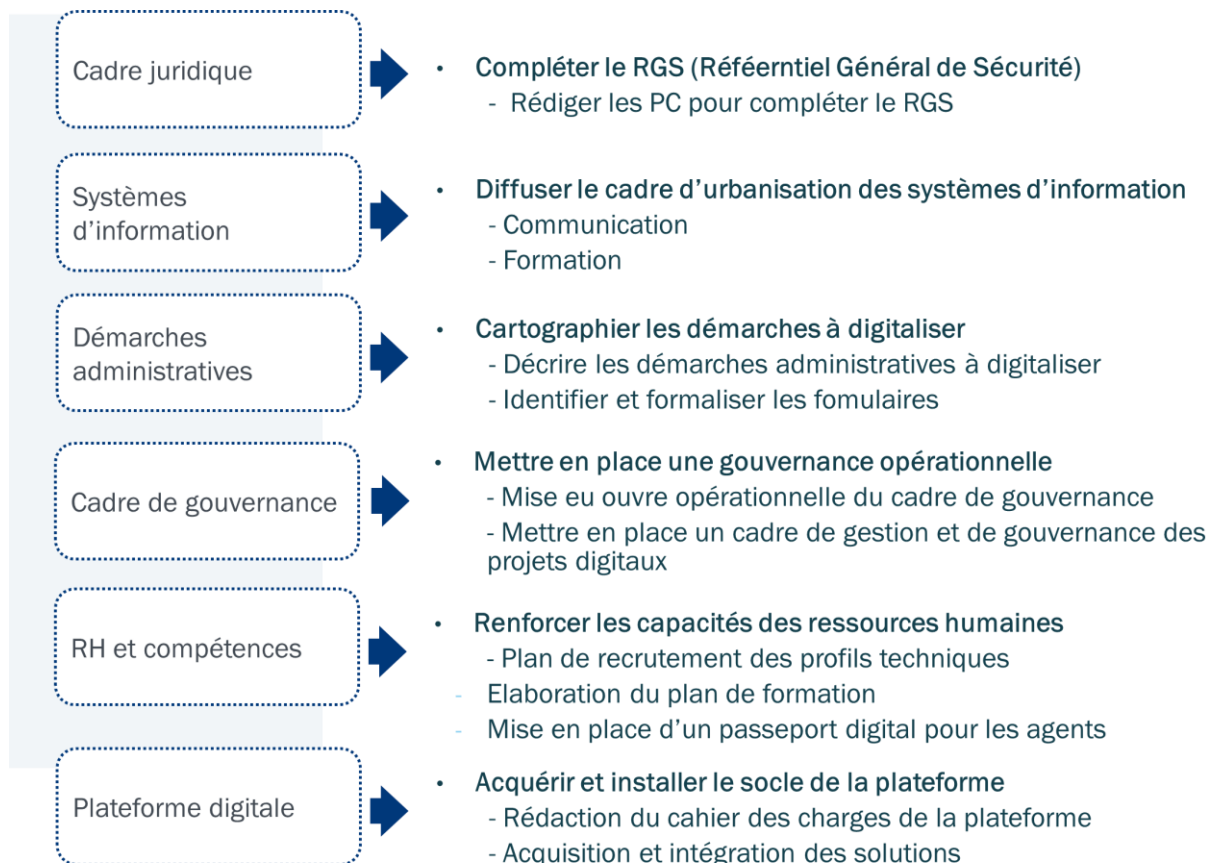
Figure 4 : Socle prioritaire de la plateforme digitale

## 6. Le plan d'actions pour mettre en œuvre le premier lot des services digitaux

La mise en œuvre des 25 services digitaux est tributaire de la réalisation des prérequis indispensables pour :

- Organiser et gouverner le programme de mise en œuvre ;
- Assurer la complétude du cadre juridique des transactions électroniques ;
- Renforcer les capacités techniques et managériales des ressources humaines ;
- Acquérir et installer le socle de la plateforme technique ;
- Développer et intégrer les services numériques.

Ainsi, la feuille de route de la mise en œuvre du premier des services digitaux en 2021 est structurée en 5 chantiers :



## 6.1. Les chantiers à lancer

### 6.1.1. Chantier 1 : Cadre juridique

<i>Domaine</i>	<i>Nom du projet</i>	<i>Priorité</i>
Cadre juridique	Compléter le RGS	1
<b>Contexte &amp; Objectifs</b>		
<ul style="list-style-type: none"><li>• Référentiel général de sécurité (RGS) trouve sa source dans le Projet de décret relatif aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives</li><li>• Le RGS, outre quelques documents d'accompagnement, peuvent comprendre des PC pour les signatures électroniques, les cachets électroniques, le chiffrement de données, l'horodatage. Ces PC présentent une importance entre eux, car ils se réfèrent au système PKI (Public Key Infrastructure).</li><li>• quelques PC peuvent être rédigées pour que le RGS devienne rapidement opérationnel</li></ul>		
<b>Pré-requis</b>		
<b>Responsable</b>		
<ul style="list-style-type: none"><li>• MESRSTIC/DGTIC</li></ul>		
<b>Contributeurs</b>		
<b>Principales activités</b>		
<ul style="list-style-type: none"><li>• Rédaction des PC « Politiques de Certification »</li><li>• Finalisation du RGS par la DGTIC</li><li>• Approbation du RGS par l'arrêté du Premier Ministre</li><li>• Publication de l'arrêté dans le Journal Officiel</li><li>• Publication en ligne du RGS</li><li>• Session de formation</li></ul>		
<b>Durée &amp; Calendrier</b>		
<ul style="list-style-type: none"><li>• 1,5 mois</li><li>• Fin décembre 2020</li></ul>		
<b>Budget estimatif</b>		
➔ 40 K€		
<b>KPI</b>		
<ul style="list-style-type: none"><li>• PC Rédigées</li><li>• RGS approuvé par arrêté du Premier Ministre publié au Journal Officiel.</li></ul>		

## 6.1.2. Chantier 2 : Systèmes d'information

<i>Domaine</i>	<i>Nom du projet</i>	<i>Priorité</i>
Systèmes d'information	Diffuser les cadres d'urbanisation des SI de l'Etat	1
<b>Contexte &amp; Objectifs</b>		
<ul style="list-style-type: none"> <li>• La DGTIC a initialisé le cadre d'urbanisation des systèmes d'information de l'Etat</li> <li>• Ce cadre devrait fournir les normes, les standards et les recommandations à suivre par les différentes administrations Mauritanienne pour mettre en œuvre leurs projets informatiques et digitaux.</li> <li>• Il est important que ces référentiels soient communiqués et appropriés par l'ensemble des administrations publiques.</li> </ul>		
<b>Pré-requis</b>		
<ul style="list-style-type: none"> <li>• Mise en place d'une gouvernance opérationnelle</li> <li>• Forte implication des responsables informatiques et SI des administrations</li> </ul>		
<b>Responsable</b>		
<ul style="list-style-type: none"> <li>• MESRSTIC/DGTIC</li> </ul>		
<b>Contributeurs</b>		
<ul style="list-style-type: none"> <li>• Tous les ministères</li> </ul>		
<b>Principales activités</b>		
<ul style="list-style-type: none"> <li>• Organiser un séminaire national pour communiquer les référentiels du cadre d'urbanisation des SI de l'Etat.</li> <li>• Elaborer un programme de formation spécifique pour accompagner les administrations à s'approprier les référentiels.</li> <li>• Publication en ligne des référentiels</li> <li>• Créer une communauté d'experts pour animer et mettre à jour les référentiels.</li> </ul>		
<b>Durée &amp; Calendrier</b>		
<ul style="list-style-type: none"> <li>• 4 mois</li> <li>• de janvier à fin avril 2021</li> </ul>		
<b>Budget estimatif</b>		
<ul style="list-style-type: none"> <li>• 10 K€</li> </ul>		
<b>KPI</b>		
<ul style="list-style-type: none"> <li>• Nombre d'administrations bénéficiaires de la formation</li> </ul>		

### 6.1.3. Chantier 3 : Démarches administratives

<i>Domaine</i>	<i>Nom du projet</i>	<i>Priorité</i>
Démarches administratives	Cartographie des démarches à digitaliser	1
<b>Contexte &amp; Objectifs</b>		
<ul style="list-style-type: none"> <li>L'analyse de l'existant a révélé l'absence de référentiel commun de démarches administratives.</li> <li>La description des processus d'une démarche administrative est un préalable pour tout projet de digitalisation.</li> </ul>		
<b>Pré-requis</b>		
<ul style="list-style-type: none"> <li>Disponibilité des textes de lois/réglementation</li> <li>Implication forte des agents publics et des directions.</li> </ul>		
<b>Responsable</b>		
<ul style="list-style-type: none"> <li>Chaque entité est responsable de l'élaboration et l'animation de son référentiel des démarches administratives.</li> </ul>		
<b>Contributeurs</b>		
<ul style="list-style-type: none"> <li>Ce référentiel doit être centralisé au niveau du MFPTMA</li> </ul>		
<b>Principales activités</b>		
<ul style="list-style-type: none"> <li>Description des démarches et des processus métier associés</li> <li>Modélisation des processus en langage standard de type BPMN</li> <li>Recueil et validation des formulaires administratifs</li> <li>Elaboration d'un référentiel des démarches</li> </ul>		
<b>Durée &amp; Calendrier</b>		
<ul style="list-style-type: none"> <li>2mois</li> <li>Novembre et décembre 2020</li> </ul>		
<b>Budget estimatif</b>		
<ul style="list-style-type: none"> <li>30 k€</li> </ul>		
<b>KPI</b>		
<ul style="list-style-type: none"> <li>Référentiel complet et à jour</li> <li>Nombre de démarches cartographiées</li> </ul>		

#### 6.1.4. Chantier 4 : Cadre de gouvernance

<i>Domaine</i>	<i>Nom du projet</i>	<i>Priorité</i>
Cadre de gouvernance	Mettre en œuvre le cadre de la gouvernance opérationnelle	1
<b>Contexte &amp; Objectifs</b>		
<ul style="list-style-type: none"> <li>• La création du Haut Conseil du Numérique ainsi que son Comité Technique permet d'apporter un dispositif de coordination concret et opérationnel représentant les principaux acteurs du paysage e-Gouvernement au niveau du pays.</li> <li>• Il est important de définir les mécanismes de gouvernance et de coordination des projets digitaux et systèmes d'information pour assurer la cohérence des initiatives et des projets à lancer par les différents ministères et établissements publics.</li> </ul>		
<b>Pré-requis</b>		
<ul style="list-style-type: none"> <li>• Lancement effectif des missions du HCN</li> <li>• Forte implication de tous les ministères</li> </ul>		
<b>Responsable</b>		
<ul style="list-style-type: none"> <li>• MESRSTIC/DGTIC</li> <li>• HCN (Haut Conseil du Numérique)</li> </ul>		
<b>Contributeurs</b>		
<ul style="list-style-type: none"> <li>• Tous les ministères</li> </ul>		
<b>Principales activités</b>		
<ul style="list-style-type: none"> <li>• Définir le fonctionnement et les mécanismes de coordination et de validation des projets digitaux à lancer</li> <li>• Définir les mécanismes et les règles de pilotage et de suivi des projets digitaux</li> <li>• Elaborer un cadre méthodologique de gestion des projets digitaux couvrant toutes les phases du cycle de vie d'un projet digital de l'étude d'opportunité jusqu'à sa fin.</li> <li>• Créer un Comité d'Architecture et de Sécurité pour contrôler le respect des règles, normes et recommandations du cadre d'urbanisation des SI.</li> <li>•</li> </ul>		
<b>Durée &amp; Calendrier</b>		
<ul style="list-style-type: none"> <li>• 3mois</li> <li>• De décembre 2020 à février 2021</li> </ul>		
<b>Budget estimatif</b>		
<b>KPI</b>		
<ul style="list-style-type: none"> <li>• Le cadre méthodologique élaboré et diffusé</li> <li>• Le Comité d'Architecture et de Sécurité est créé.</li> </ul>		

## 6.1.5. Chantier 5 : Renforcement des capacités

<i>Domaine</i>	<i>Nom du projet</i>	<i>Priorité</i>
RH et compétences	Renforcer les capacités des ressources humaines	1
<b>Contexte &amp; Objectifs</b>		
<ul style="list-style-type: none"> <li>L'analyse e l'existant a pointé un fort besoin de renforcement des capacités des ministères (très faible nombre de profils techniques, absence de politique de formation structurée, manque de certaines compétences clés comme les experts en sécurité et en architecture, etc...)</li> <li>La mise à niveau du capital humain de l'administration Mauritanienne et la diffusion de la culture digitale au près des agents publics sont des prérequis pour réussir la digitalisation des services publics en Mauritanie.</li> </ul>		
<b>Pré-requis</b>		
<ul style="list-style-type: none"> <li>Mise en place d'une gouvernance opérationnelle</li> <li>Forte implication des responsables informatiques et SI des administrations</li> </ul>		
<b>Responsable</b>		
<ul style="list-style-type: none"> <li>MFPTMA</li> </ul>		
<b>Contributeurs</b>		
<ul style="list-style-type: none"> <li>Tous les ministères</li> </ul>		
<b>Principales activités</b>		
<ul style="list-style-type: none"> <li>Définir les besoins de recrutement des profils techniques (experts en sécurité, architectes SI, chefs de projet, etc...);</li> <li>Elaboration d'un plan de formation dédié aux agents des directions informatiques et DSIs (sécurité numérique, gestion des projets, architecture SI, projets agiles, gestion des infrastructures numériques, accompagnement au changement, etc...)</li> <li>Elaboration d'un passeport digital de l'agent pour accompagner les utilisateurs internes à mieux s'approprier les services digitaux.</li> <li></li> </ul>		
<b>Durée &amp; Calendrier</b>		
<ul style="list-style-type: none"> <li>12mois</li> <li>De janvier à décembre 2021</li> </ul>		
<b>Budget estimatif</b>		
<b>KPI</b>		
<ul style="list-style-type: none"> <li>Nombre de recrutement</li> <li>Nombre de passeports digitaux délivrés</li> <li>Nombre d(agents techniques bénéficiaires des formations techniques.</li> <li>Nombre d'agents publics ayant obtenus des certifications techniques (PMI, Sécurité, Scrum Master, ITIL, COBIT, etc...)</li> </ul>		

## 6.1.6. Chantier 6 : Plateforme digitale

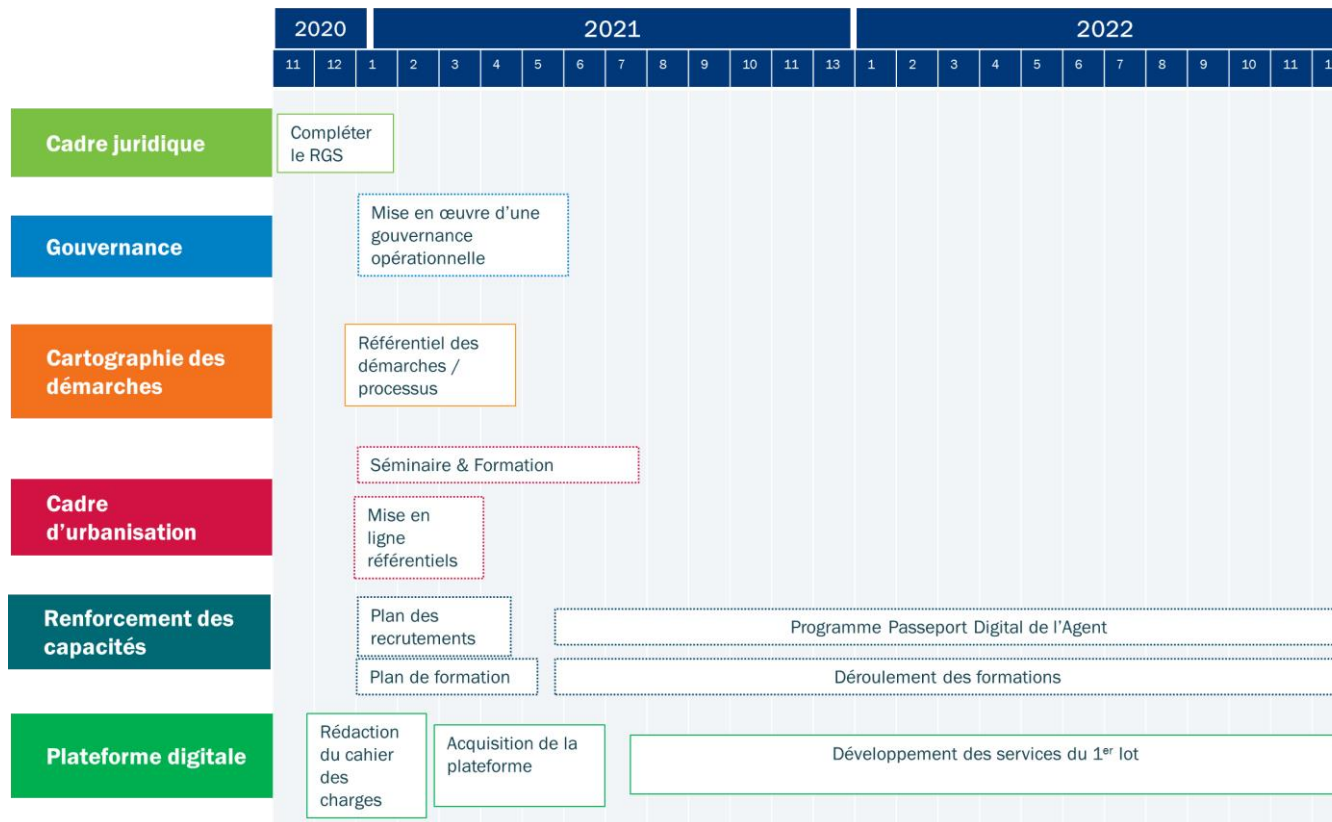
<i>Domaine</i>	<i>Nom du projet</i>	<i>Priorité</i>
Plateforme technique	Rédiger le cahier des charges de la plateforme technique	1
<b>Contexte &amp; Objectifs</b>		
<ul style="list-style-type: none"> <li>• L'étude de cadrage et de faisabilité a permis de définir l'architecture fonctionnelle et technique de la plateforme de digitalisation.</li> <li>• Pour déployer cette plateforme, un cahier des charges détaillant les briques fonctionnelles et techniques de la plateforme est à produire.</li> </ul>		
<b>Pré-requis</b>		
<ul style="list-style-type: none"> <li>• Validation du cahier des charges</li> <li>• Engagement des entités bénéficiaires du programme de digitalisation.</li> </ul>		
<b>Responsable</b>		
<ul style="list-style-type: none"> <li>• MESRSTIC/DGTIC</li> </ul>		
<b>Contributeurs</b>		
<ul style="list-style-type: none"> <li>• Tous les ministères</li> </ul>		
<b>Principales activités</b>		
<ul style="list-style-type: none"> <li>• Mettre en place un comité technique à piloter par la DGTIC (un représentant technique de chaque entité administrative bénéficiaire);</li> <li>• Recrutement d'un Consultant pour rédiger le cahier des charges;</li> <li>• Elaboration du cahier des charges incluant : les spécifications techniques et fonctionnelles des briques de la plateforme, la description des services à digitaliser, les exigences qualité et calendaires à respecter.</li> <li>•</li> </ul>		
<b>Durée &amp; Calendrier</b>		
<ul style="list-style-type: none"> <li>• 1,5 mois</li> <li>• Novembre et décembre 2020</li> </ul>		
<b>Budget estimatif</b>		
<ul style="list-style-type: none"> <li>• 60 K€</li> </ul>		
<b>KPI</b>		
<ul style="list-style-type: none"> <li>• Cahier des charges rédigé et validé</li> <li>•</li> </ul>		

<i>Domaine</i>	<i>Nom du projet</i>	<i>Priorité</i>
Plateforme technique	Acquérir et installer le socle de la plateforme technique Développer le 1 <sup>er</sup> de lot de services	1
<b>Contexte &amp; Objectifs</b>		
<ul style="list-style-type: none"> <li>• L'étude de cadrage et de faisabilité a permis de définir l'architecture fonctionnelle et technique de la plateforme de digitalisation.</li> <li>• L'étude a également identifié le Ar de services digitaux à mettre en œuvre en 2021.</li> <li>• Le développement de ce premier lot des services sera l'occasion de déployer un première instanciation de la plateforme digitale.</li> </ul>		
<b>Pré-requis</b>		
<ul style="list-style-type: none"> <li>• Validation de l'étude de faisabilité</li> <li>• Rédaction et validation du cahier des charges</li> <li>• Lancement de la consultation</li> <li>• Engagement des entités bénéficiaires du programme de digitalisation.</li> </ul>		
<b>Responsable</b>		
<ul style="list-style-type: none"> <li>• MESRSTIC/DGTIC</li> </ul>		
<b>Contributeurs</b>		
<ul style="list-style-type: none"> <li>• Tous les ministères</li> </ul>		
<b>Principales activités</b>		
<ul style="list-style-type: none"> <li>• Mise en place d'une structure de gouvernance spécifique du programme</li> <li>• Acquisition et intégration des briques prioritaires : plateforme portail et workflow management, plateforme API, plateforme de gestion d'identité, plateforme de supervision, plateforme de business intelligence</li> <li>• Développement du 1<sup>er</sup> lot des services digitaux (état civil et papiers d'identité, plateforme RDV, portail paiement, demande de casier judiciaire, demande de permis de construire, espace étudiant, espace agent public, démarches CNSS, demande de visa, Inscription aux concours)</li> </ul>		
<b>Durée &amp; Calendrier</b>		
<ul style="list-style-type: none"> <li>• 24 mois</li> <li>• 6 mois : Acquisition</li> <li>• 18 mois : installation et développement des services.</li> </ul>		
<b>Budget estimatif</b>		
<ul style="list-style-type: none"> <li>• 3 530 K€</li> </ul>		
<b>KPI</b>		
<ul style="list-style-type: none"> <li>• Plateforme acquise et intégrée</li> <li>• Nombre de services digitalisés</li> <li>•</li> </ul>		

## 6.2. Le calendrier

Afin d'arriver à mettre en œuvre les 23 services digitaux en 2021, nous proposons un calendrier structuré autour des principaux jalons suivants :

- Fin Décembre 2020 : Préparer les prérequis juridiques et organisationnels et élaborer le cahier des charges de la plateforme
- Fin Mars 2021 : Acquérir la solution technique
- A partir d'Avril 2021 : Démarrer le développement des services digitaux.



### 6.3. Le budget estimatif

Le budget estimatif présenté ci-dessous couvre les éléments suivants :

- Finalisation des prérequis juridiques ;
- Rédaction du cahier des charges de la plateforme ;
- Acquisition et intégration du premier socle de la plateforme ;
- Développement des 23 services numériques ;
- Développement des APIs.

	Budget estimatif de 2021	Budget estimatif de 2022
Rédaction du cahier des charges, Rédaction RGS, Cartographie des processus	120	
Acquisition et intégration des briques prioritaires	680	
Plateforme workflow/BPM + portail	100	
Plateforme BI	80	
Plateforme API	100	
Plateforme Identité (IAM)	150	
Plateforme supervision	50	
Coffre-fort électronique	150	
Mise à niveau de l'infrastructure d'hébergement	50	
Développement & intégration des services du 1er lot	840	1360
Développement des APIs	100	100

AMOA, formation et accompagnement	250	200
-----------------------------------	-----	-----

<b>Budget Total</b>	<b>1990</b>	<b>1660</b>
---------------------	-------------	-------------

### HYPOTHESES DE CALCUL DES COÛTS DE DEVELOPPEMENT ET D'INTEGRATION DES 25 SERVICES DU PREMIER LOT

Le calcul du budget estimatif de développement et d'intégration des services est basé sur le niveau de la complexité fonctionnelle de chaque service.

Les services sont ainsi classés en :

- Simples
- Moyens
- Complexes

L'estimation des coûts est basée sur les abaques suivants :

Niveau de complexité du service	Coût Conception/Dev
Simple	60 K€
Moyen	100 K€
Complexe	200 K€

Service	Ministères & entités	Nombre de services	Complexité Faible	Complexité Moyenne	Complexité Forte
Etat civil et papiers d'identité	MIDEC/ AN-RPTS	3	3		

Service	Ministères & entités	Nombre de services	Complexité Faible	Complexité Moyenne	Complexité Forte
Casier judiciaire	MJ	1	1		
inscription aux concours	MFPTMA & MESRSTIC	1		1	
Permis de construire	MHUAT, MI-DEC, Mairie, MF	1		1	
Démarches CNSS	CNSS	4	2	1	1
Plateforme RDV	MESRSTIC	1		1	
Paiement	MESRSTIC, GIMTEL, MF	1		1	
demande de visa	MIDEC / AN-RPTS	1		1	
Espace étudiant	MESRSTIC	5	3	2	
Espace Agent	MFPTMA	5	2	3	

Service	Ministères & entités	Nombre de services	Complexité Faible	Complexité Moyenne	Complexité Forte
Demande des autorisation et des agréments	Guichet Unique	2		2	

## HYPOTHESES DE CALCUL DES COÛTS DE DEVELOPPEMENT DES API

Le calcul du budget estimatif de développement des APIs est basé sur le niveau de complexité de l'interface.

Niveau de complexité de l'API	Coût Conception/Dev
Simple	2,5 K€
Moyen	5 K€
Complexe	10 K€

Service	Ministères & entités	Nombre de services	Nbre API	API simples	API moyens	API complexes
Etat civil et papiers d'identité	MIDEC/ AN-RPTS	3	3		3	
Casier judiciaire	MJ	1	1		1	

Service	Ministères & entités	Nombre de services	Nbre API	API simples	API moyens	API complexes
inscription aux concours	MFPTMA & MESRSTIC	1	2		2	
Permis de construire	MHUAT, MIDEDEC, Mairie, MF	1	2		2	
Démarches CNSS	CNSS	4	6	2	2	2
Plateforme RDV	MESRSTIC	1	2	1	1	
Paiement	MESRSTIC, GIMTEL, MF	1	2		1	1
demande de visa	MIDEDEC / ANRPTS	1	2	1	1	
Espace étudiant	MESRSTIC	5	5	3	2	
Espace Agent	MFPTMA	5	5	3	2	
Demande des autorisations et des agréments	Guichet Unique	2	5			5



## 7. Annexes

### 7.1. Les scénarii de digitalisation des paiements publics en Mauritanie

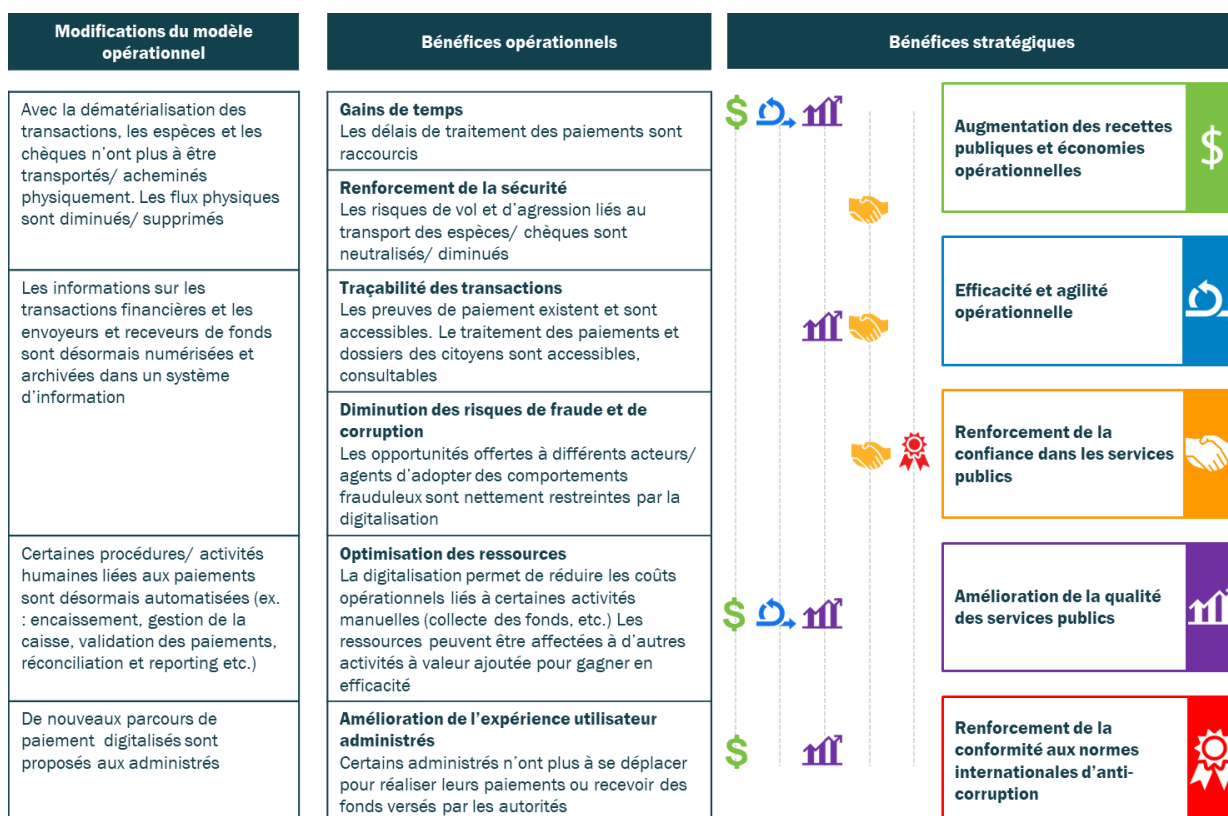
#### I. La digitalisation des paiements gouvernementaux, axe stratégique d'un projet de digitalisation des services publics

##### 1. Dématérialiser les paiements

La digitalisation des paiements gouvernementaux repose sur la mise en place de systèmes permettant de numériser tout ou partie des chaînes de paiement relatives aux encaissements et décaissements réalisés par des entités publiques mauritaniennes. Cela se traduit concrètement par le remplacement des paiements en espèces ou par chèques par des paiements par carte, virement ou via du mobile money.

De nombreux pays tels que la Côte d'Ivoire, le Sénégal ou l'Égypte par exemple se sont ainsi engagés dans la voie de la digitalisation des paiements réalisés par les entités publiques, afin de capitaliser sur les nombreux bénéfices offerts par cette démarche.

##### 2. Favoriser une croissance inclusive en exploitant le gisement de bénéfices stratégiques offerts par la digitalisation des paiements gouvernementaux



## *Bénéfices opérationnels et stratégiques de la digitalisation des paiements*

La digitalisation des paiements gouvernementaux offre de nombreux bénéfices à l'Etat et aux administrés orientés autour de 5 axes :

- **Augmentation des recettes publiques et économies de coûts**

En réduisant le nombre de tâches et activités manuelles (collecte de fonds, etc.) grâce à l'automatisation offerte par la digitalisation, le gouvernement peut économiser jusqu'à 75% de ses coûts opérationnels<sup>1</sup>. Les administrés bénéficient également d'économies de coûts en limitant leur déplacement en utilisant le paiement à distance. Les déplacements économisés ainsi que les délais de traitement d'opérations plus courts constituent un gain de temps considérable qui peut également être un facteur d'adoption du service, permettant d'augmenter le nombre de paiements collectés et ainsi accroître les recettes publiques. La traçabilité des opérations et la diminution des risques de vol et de fraude grâce à la dématérialisation des transactions permettent également d'augmenter les recettes publiques.

- **Transformation structurelle favorisant l'efficacité et l'agilité opérationnelle**

Grâce à l'automatisation de certaines procédures et activités humaines liées aux paiements (encaissement, gestion de la caisse, validation des paiements, réconciliation et reporting etc.), les ressources sont optimisées puisqu'elles peuvent désormais être affectées à d'autres activités à valeur ajoutée pour gagner en efficacité.

- **Amélioration de la qualité des services publics et renforcement de la confiance**

L'expérience utilisateur des administrés est améliorée grâce à la mise en place de nouveaux parcours digitalisés, limitant ainsi leur déplacement et offrant des délais de traitement plus courts. De plus, la digitalisation permet de numériser et d'archiver les transactions financières dans un système d'information apportant plus de traçabilité et diminuant les risques de fraude et de corruption. Les administrés ont accès à leur dossier et reçoivent une preuve de paiement ce qui renforce leur confiance dans les services publics.

- **Meilleure mise en application des normes internationales de lutte contre la corruption**

La digitalisation restreint les opportunités offertes à différents acteurs ou agents d'adopter des comportements frauduleux.

- **Développement de l'inclusion financière**

La digitalisation des paiements gouvernementaux permet de favoriser l'inclusion financière. En effet l'adoption du paiement digital par les administrés repose sur l'accessibilité accrue aux services financiers formels. En offrant plusieurs moyens de paiements et en formalisant des processus de paiement digitaux, le gouvernement a la possibilité d'encourager l'adoption de services financiers formels et digitaux auprès de ses administrés.

---

<sup>1</sup> Numérisation des paiements : des gisements de croissance et de développement inclusif, BTCA, 2018

## II. Différents modèles de digitalisation des paiements gouvernementaux peuvent être adoptés

### 1. Implémenter la digitalisation des paiements gouvernementaux : des modèles bâtis autour de trois composantes essentielles

Les modèles de digitalisation des paiements sont bâtis autour de trois briques essentielles :

- Les interfaces utilisateurs : elles sont les points de contacts au travers desquelles les citoyens réalisent les paiements. Elles peuvent être physiques (guichets) ou digitales (canaux web, applications mobiles etc.)
- Les instruments de paiement : ils sont les moyens de paiement utilisés par les administrés pour effectuer ou recevoir les paiements. Ils peuvent être de nature physique comme les espèces ou les chèques par exemple, ou bien dématérialisée tels que le virement ou la monnaie électronique.
- L'infrastructure : elle est la composante « back end » du modèle, celle qui permet d'interconnecter les SI, notamment les SI des administrations, et les acteurs du modèle de paiement.

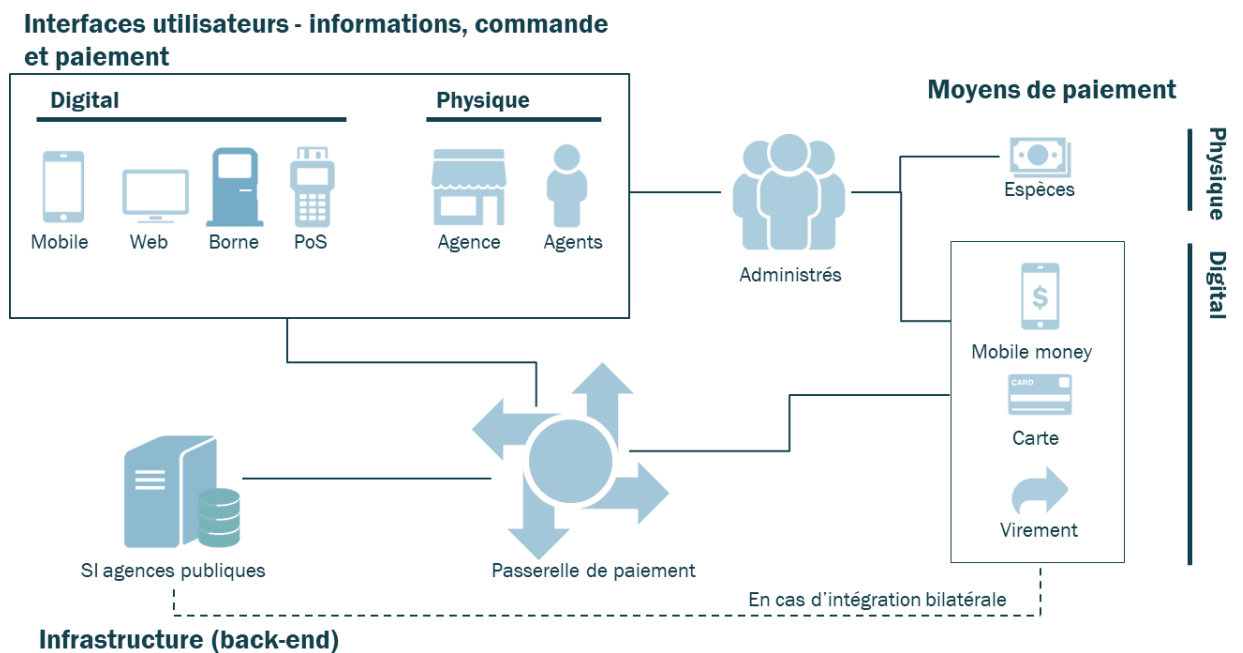


Schéma de digitalisation des paiements

### 2. Parmi une multitude de variantes, trois modèles principaux émergent

En s'appuyant sur les trois composantes principales du modèle de digitalisation et en analysant les modèles existants dans d'autres pays, nous avons défini trois principaux modèles de digitalisation des paiements publics.

#### Modèle « digital fermé »

Il est construit autour d'un opérateur de mobile money qui propose le paiement de services publics sur ses propres canaux. Les interfaces sont digitales<sup>2</sup> et sont proposées par le fournisseur de l'instrument de paiement : l'utilisateur interagit via une application mobile ou un menu USSD. En plus de contrôler l'instrument de paiement et les interfaces, le fournisseur de l'instrument de paiement gère également la partie infrastructure puisqu'il met à disposition son système de paiement auquel peuvent s'interconnecter de façon bilatérale les entités publiques. Ce modèle est présent notamment en Côte d'Ivoire, où le Ministère de l'Education Nationale et de l'Enseignement Technique (MENET) a décidé de créer un système de paiement digital permettant de payer les frais d'inscription à distance. Le MENET s'est appuyé dans un premier temps sur le service de mobile money de l'opérateur MTN et son réseau de distribution avant de s'étendre aux autres opérateurs de télécommunications du pays (Orange et Moov). Les usagers effectuent ainsi le paiement des frais de scolarité en utilisant un service de mobile money ou au travers du réseau de distribution des opérateurs. Le Ministère prend alors en charge le règlement des frais de commission des agents lors des opérations de dépôts (cf. livrable 1). Dans ce modèle, l'opérateur du service de paiement fournit ainsi l'essentiel du dispositif via l'interface et l'instrument de paiement lui-même. Le dispositif est dit en « boucle fermée » (« closed loop ») : autorités et administrés doivent disposer d'un compte mobile money chez cet opérateur pour réaliser ces paiements.

### **Modèle « digital délégué à une passerelle de paiement »**

Le deuxième modèle repose sur un fournisseur d'une passerelle de paiement (« payment gateway ») mettant à disposition son infrastructure ainsi que des interfaces digitales qu'il contrôle également. L'utilisateur a le choix entre les différents types et fournisseurs d'instruments de paiement qui sont acceptés par la passerelle de paiement : mobile money, virement, cartes bancaires locales ou internationales. Les différents services de paiement et les SI des entités publiques sont interconnectés via cette passerelle de paiement.

Ce modèle a été mis en place notamment au Sénégal par la Sénégalaise des Eaux (SDE) pour le paiement de facture d'eau en s'appuyant sur la plateforme Orbus fournie par l'entreprise Gainde2000. Ainsi, Gainde2000 met à disposition de la SDE un portail de paiement. Gainde2000 concentre plusieurs services de paiement au travers de sa plateforme tels que : Orange Money et Tigo Cash pour le mobile money, les cartes Visa et Mastercard, etc. Ainsi, la SDE, en s'interconnectant à la plateforme Orbus, délègue toute la gestion des paiements à Gainde et permet à ses usagers, au travers des interfaces proposées par Gainde, de payer via une multiplicité de moyens de paiements.

### **Modèle « digital full control »**

Le troisième modèle repose sur un contrôle fort des entités publiques sur le modèle, à la fois sur les canaux proposés et l'infrastructure de paiement. L'administration met à disposition des usagers

---

<sup>2</sup> Interface digitale : point d'interaction numérique nomade entre une personne et un système – il ne requiert pas de déplacement dans un lieu spécifique (ex : portail web, application mobile, portail USSD)

Interface phygitale : point d'interaction numérique entre un utilisateur et un système qui requiert un déplacement dans un lieu spécifique (ex : GAB, TPE, borne de service)

Interface physique : point d'interaction entre un utilisateur et un système qui requiert un déplacement dans un lieu spécifique et l'intervention d'une seconde personne servant d'intermédiaire

ses propres interfaces digitales (web, application mobile ou USSD). L'utilisateur réalise toutes les opérations sur la même interface, de la « commande » au paiement. Les administrations contrôlent également l'infrastructure de paiement : elle est certes fournie par un tiers (fournisseur de passerelle de paiement) mais elle est encadrée par un dispositif de sous-traitance, qui laisse à l'entité publique le contrôle de cette composante. Grâce à cette passerelle, plusieurs instruments de paiement digitaux (mobile money, virement) et électroniques (cartes bancaires locales et internationales), proposés par les fournisseurs qui se sont interfacés à la passerelle de paiement, sont disponibles. Les systèmes d'information des entités publiques sont également directement intégrés à la passerelle de paiement. Le gouvernement a ainsi une visibilité et une maîtrise de la solution dans son ensemble.

		<b>Non digitalisé</b>		<b>Digital « fermé » : mobile money led</b>		<b>Digital délégué à une passerelle de paiement</b>		<b>Digital full control</b>	
		Le paiement de services publics ne peut se faire via des canaux et instruments digitaux		Un opérateur mobile money propose le paiement de services publics sur ses propres canaux		Un fournisseur de payment gateway propose le paiement de services publics sur des canaux digitaux qu'il contrôle		Les entités publiques proposent le paiement sur leurs propres canaux en s'appuyant sur une passerelle de paiement	
1	Interfaces digitales	Non	Propriété : entités publiques	• App mobile • USSD	Propriété : tiers (fournissr. instrument de paiement)	• Web • App mobile	Contrôle : fournisseur passerelle de paiement	• Web • App mobile • USSD	Contrôle : entités publiques
	Interfaces phygtales	Non		Non		Non			
	Interfaces physiques	• Guichets		Non		Non			
	Interface unique commande et paiement	Le plus souvent (formalités et paiement simultanés au guichet)		Non	Non	Oui			
2	Inst. paiement digitaux	Non		• Mobile money	1 inst. paiement unique ou liste fermée instrumts	• Mobile money • Virement	Ouverts aux inst. paiement généralemt acceptés localement	• Mobile money • Virement	Ouverts aux inst. paiement généralemt acceptés localement
	Inst. paiement élec.	Non		Non		• Carte banc. locale • Carte banc. internat.		• Carte banc. locale • Carte banc. internat.	
	Inst. paiement physique	• Espèces • Chèques		Non	Non	Non			
3	SI public intégré avec inst. paiement	Non applicable		Non ou en bilatéral		Via une passerelle de paiement		Via une passerelle de paiement	
	Contrôle infra. paiement	Non applicable		Tiers (fournisseur inst. de paiement)		Fournisseur de la passerelle de paiement		Entités publiques, sous-traité fourniss. passerelle de paiement	

Caractérisation des principaux modèles de digitalisation

### **3. Dans le contexte mauritanien nous préconisons une digitalisation des paiements gouvernementaux en deux temps : mise en place d'un modèle « digital délégué à une passerelle de paiement » qui nécessite dans un premier temps un modèle de transition « phygital »**

- 1. Dans le contexte mauritanien, le cadre réglementaire joue un rôle essentiel dans le développement et l'adoption des services financiers digitaux qui pourront s'appuyer sur une infrastructure existante**

#### **Une offre de services financiers digitaux limitée à cause d'un contexte réglementaire peu favorable...**

L'absence de cadre réglementaire sur les paiements digitaux et l'inexistence d'une infrastructure de paiements mobiles ne favorisent pas le développement d'une offre de services et de moyens de paiements digitaux. En effet, la Mauritanie s'est dotée d'un régime encadrant les virements et paiements par cartes « électroniques ». En revanche, il n'encadre pas les services financiers digitaux, notamment les services de paiement mobile et de monnaie électronique et réserve l'émission d'instruments de paiement électroniques aux seules institutions financières (cf. livrable 1). Ainsi, seul Bankily, service financier digital lancé en 2019 par la Banque Populaire de Mauritanie en partenariat avec Mattel, semble être actif, ce qui limite l'adoption et la diffusion des services financiers digitaux dans le pays.

#### **... limitant l'accès aux services financiers formels à la population mauritanienne**

L'accès aux services financiers formels est faible puisque seulement 21% des adultes âgés de 15 ans et plus possédaient un compte dans une institution financière ou un compte de mobile money en 2017 (cf. livrable 1). Cela incite la population à utiliser essentiellement des espèces pour réaliser des paiements ou des transferts d'argent, en s'appuyant sur des acteurs financiers informels. De plus, la faible adoption des services de paiements digitaux peut également s'expliquer par une méconnaissance du digital et une faible maturité client sur le sujet (cf. livrable 1).

#### **Néanmoins les services financiers digitaux sont appelés à se développer notamment grâce à la mise en place d'un cadre réglementaire dédié**

La mise en place d'un cadre réglementaire est un enjeu fort pour le développement des services financiers digitaux en Mauritanie. L'élaboration d'une Stratégie Nationale d'Inclusion Financière (SNIF) couplée à l'entrée en vigueur de lois régissant le paiement électronique et l'ouverture du marché à des acteurs autres que les banques sont les principaux catalyseurs du développement des services financiers digitaux. La Mauritanie possède également d'autres atouts puisqu'elle est dotée d'une infrastructure de paiement existante et de réseaux d'agents tels que ceux des opérateurs de transfert de fonds, offrant une bonne capillarité pour rendre accessible les SFD. La population mauritanienne a régulièrement recours aux services de transfert d'argent des opérateurs de transfert de fonds ce qui témoigne d'une certaine éducation financière. Ces caractéristiques associées à un taux d'adoption important de la téléphonie mobile et de l'internet mobile, ainsi que le pourcentage très élevé de la population possédant des documents d'identité (cf. livrable 1), rend favorable le développement et l'adoption des SFD en Mauritanie.

#### **Une multiplicité d'instruments de paiement facilite l'adoption des paiements digitaux par les administrés et permet au gouvernement de ne pas dépendre d'un seul fournisseur d'instrument de paiement**

Afin de favoriser l'adoption du service, il est essentiel de proposer aux administrés une multiplicité d'instruments de paiement pour couvrir tous les besoins et développer l'usage des paiements dématérialisés. En Mauritanie, la carte bancaire, bien que reposant sur l'infrastructure interopérable du GIMTEL, ne couvrait en 2017 que 10% des adultes âgés de 15 ans et plus en carte de débit et 3% en carte de crédit (Banque Mondiale) (cf. livrable 1). Un modèle de digitalisation des paiements

gouvernementaux basé uniquement sur un paiement par carte ne toucherait qu'une faible partie de la population (environ 277 000 personnes).

De plus, en s'appuyant sur un seul fournisseur d'instrument de paiement, le gouvernement est dépendant d'un unique acteur sur plusieurs aspects critiques tels que la disponibilité de la solution, l'évolutivité ou les failles techniques.

La multiplication des instruments de paiements disponibles et l'accessibilité à différents fournisseurs de services de paiement, permet d'assurer une fiabilité technique et d'atteindre une plus grande part de la population, favorisant ainsi la diffusion à plus grande échelle de la digitalisation des paiements.

### **La plateforme du GIMTEL permet de s'appuyer sur une infrastructure existante offrant de l'interopérabilité bancaire et évoluant vers l'intégration de nouveaux instruments de paiement digitaux et mobiles**

En Mauritanie, une infrastructure de paiement est déjà en place. En effet, le GIMTEL a mis en place un switch supportant l'interbancaire des paiements électroniques par carte, sur lequel toutes les banques du pays sont connectées. Par ailleurs, depuis mai 2020, le GIMTEL a lancé une plateforme nationale de paiement en ligne permettant à tout marchand d'accepter les paiements en ligne par cartes GIMTEL, Visa et Mastercard. Cette plateforme intègre la norme 3D Secure afin d'assurer la sécurité des opérations.

Le GIMTEL prévoit également la mise en place d'une plateforme de paiement mobile interopérable. Cette plateforme, qui servira de hub de paiement mobile pour tous les fournisseurs, proposera l'interopérabilité des paiements par mobile.

En s'appuyant sur les plateformes de paiement du GIMTEL, le gouvernement peut ainsi capitaliser sur une infrastructure existante et évolutive pour mettre en œuvre la digitalisation des paiements gouvernementaux.

## **2. Nous avons établi une liste de critères permettant d'évaluer la pertinence d'un modèle de digitalisation des paiements**

Dans le but d'évaluer la pertinence des différents scénarios de digitalisation des paiements, nous avons identifié 4 critères d'évaluation.

<b>Critère d'évaluation</b>	<b>Description</b>
<b>Niveau de couverture</b>	Niveau de couverture de la population d'administrés par la solution.  <i>Ce critère mesure la taille de la population d'administrés adressable par la solution cible. Il prend notamment en compte le niveau d'adéquation entre la solution et les usages des administrés ainsi que la capacité de la solution à intégrer des moyens de paiement variés</i>
<b>Expérience client</b>	Qualité de l'expérience de paiement pour les administrés.  <i>Ce critère prend en compte le type et le nombre de canaux utilisés ainsi que l'ergonomie et l'accessibilité des interfaces de la solution cible. Il prend également en considération le niveau de contrôle du gouvernement sur l'expérience client</i>
<b>Mise en œuvre et gestion</b>	Niveau de complexité global de la solution.

Critère d'évaluation	Description
	<i>Ce critère prend en compte la capacité du gouvernement, de ses agences et des fournisseurs de paiement à mettre en œuvre le modèle cible. Ce critère prend également en considération le niveau d'effort à fournir par le gouvernement pour la gestion opérationnelle de la solution cible.</i>
<b>Investissement</b>	Niveau d'investissement initial requis pour mettre en place la solution cible.  <i>Ce critère prend principalement en compte les investissements liés à l'infrastructure, au développement et à l'intégration de la solution cible.</i>

*Critères d'évaluation d'un modèle de digitalisation des paiements*

3. Sur la base de ces critères, le scénario « Digital délégué à une passerelle de paiement » semble le plus adapté

Critère d'évaluation	(1) Digital « fermé »	(2) Digital « délégué à une passerelle de paiement »	(3) Digital « full control »
Niveau de couverture	1	3	3
Expérience client	1	2	3
Mise en œuvre et gestion	3	2	1
Investissement	3	3	1

*Grille d'évaluation des modèles de digitalisation des paiements envisagés*



**(1) Digital « fermé » : un modèle de dépendance trop fort pour un gouvernement et qui présente peu d'intérêt pour les administrés mauritaniens**

Ce scénario repose sur l'externalisation de la gestion du paiement à un unique opérateur de mobile money. Cela permet de réduire grandement l'investissement initial requis. Les coûts liés à l'acquisition d'une infrastructure de paiement, le développement d'interfaces digitales et l'intégration sont assumés par l'opérateur de mobile money. La mise en œuvre et la gestion de la solution sont confiées à l'opérateur de mobile ce qui réduit considérablement les efforts à mettre en œuvre et les ressources dédiées du côté du gouvernement.

Néanmoins, dans ce dispositif seul un instrument de paiement est disponible auprès d'un unique opérateur de mobile money. Ce monopole est un frein au développement des paiements digitalisés entre le gouvernement et les administrés car le succès du modèle repose en grande partie sur l'adoption du service de l'opérateur de mobile money. Par ailleurs, dans ce cas de figure, l'opérateur de mobile money est propriétaire des interfaces digitales ce qui offre au gouvernement peu de contrôle sur la qualité de l'expérience et des parcours clients. Enfin,

la passerelle de paiement n'étant pas forcément intégrée au SI du gouvernement, cette solution ne permet pas de proposer un parcours utilisateur sans couture.

Ce modèle présente par ailleurs un désavantage majeur, celui de la dépendance à un unique fournisseur d'instrument de paiement. D'une part, l'équilibre de la concurrence peut s'en trouver faussé. D'autre part en cas de faille critique de l'unique fournisseur d'instrument de paiement le système de paiement se trouve paralysé.

### **(2) Digital « délégué à une passerelle de paiement » : un modèle peu coûteux et propice à l'adoption des paiements digitaux**

Dans ce scénario les coûts sont principalement supportés par le fournisseur de la passerelle de paiements qui gère à la fois l'infrastructure et les interfaces digitales. Le gouvernement supporte un niveau de coûts limité lié à l'intégration de ses SI avec la passerelle de paiements. Par ailleurs, la gestion de la solution et l'intégration de nouveaux instruments de paiements sont également confiées au fournisseur de la passerelle ce qui limite les efforts de mise en œuvre et d'exploitation de la solution du côté du gouvernement. C'est le fournisseur de la passerelle de paiement qui possède les compétences et l'expérience nécessaire à la gestion de la solution. Pour mettre en œuvre ce dispositif, le gouvernement peut s'appuyer sur l'infrastructure du GIMTEL qui propose déjà une passerelle de paiements fonctionnelle.

La force de ce dispositif réside dans la diversité des fournisseurs d'instruments de paiements qui sont intégrés. C'est un système « ouvert » qui permet d'intégrer plusieurs types d'instruments (ex : cartes de paiement nationales, cartes de paiement internationales et mobile money) et plusieurs fournisseurs (ex : toutes les banques, tous les opérateurs de mobile money). La diversité des instruments de paiements et des fournisseurs intégrés permet d'adresser une plus grande partie de la population et, par conséquent, de faciliter l'adoption de la solution de digitalisation des paiements gouvernementaux. Par ailleurs, comme dans le modèle (1), le fournisseur de la passerelle de paiement est propriétaire des interfaces digitales ce qui offre peu de contrôle au gouvernement sur les parcours utilisateurs. Toutefois, dans ce scénario, la passerelle de paiement est directement intégrée au SI du gouvernement ce qui suppose une meilleure qualité de l'expérience utilisateur.

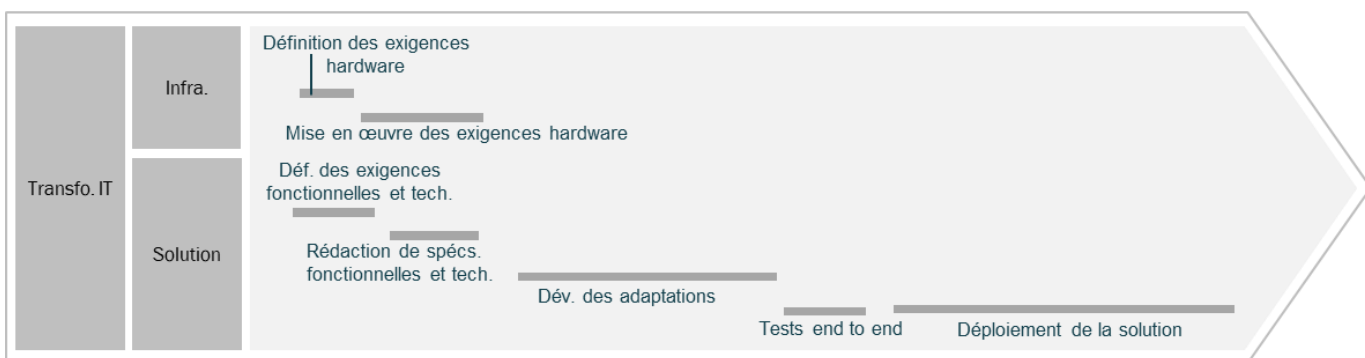
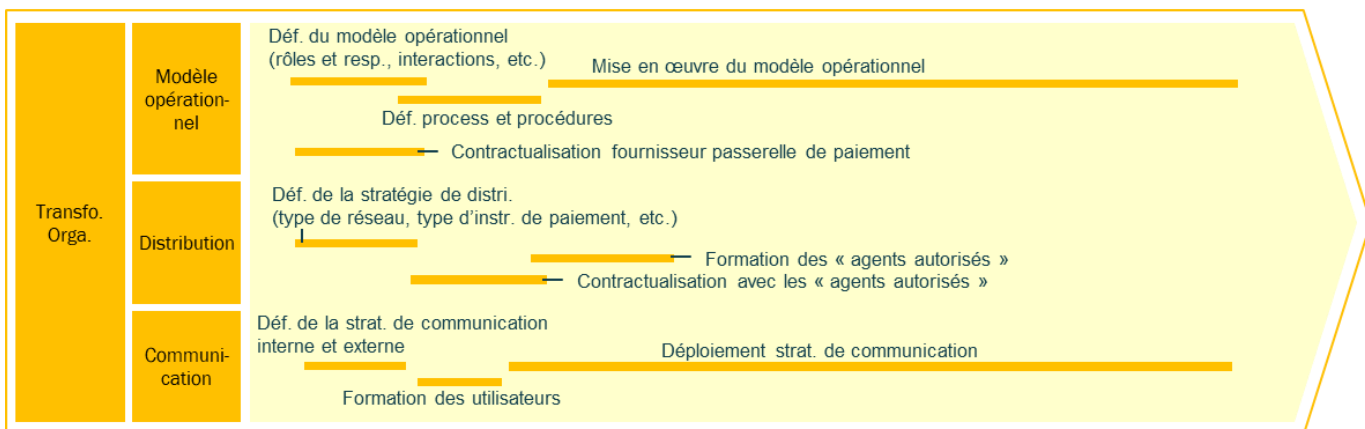
### **(3) Digital « full control » : un scénario coûteux qui requiert des ressources, des compétences et des efforts considérables pour le gouvernement**

Dans ce modèle, l'ensemble des interfaces de paiement appartiennent au gouvernement ce qui implique des niveaux de coûts plus élevés que dans les autres modèles. Le gouvernement supporte par ailleurs des coûts liés à l'intégration de son SI avec le fournisseur de la passerelle de paiement. En termes de mise en œuvre et de gestion, des efforts considérables sont requis du côté du gouvernement qui doit gérer les interfaces digitales et leur intégration avec la passerelle de paiement.

Tout comme le modèle (2) ce dispositif, permet d'intégrer plusieurs types d'instruments de paiement proposés par plusieurs fournisseurs différents. Cela permet d'adresser une plus grande partie de la population et de faciliter l'adoption de la solution. Le principal avantage de ce modèle réside dans l'expérience client. En effet, dans ce scénario le gouvernement a un contrôle quasi total sur les parcours client et peut donc les optimiser et les uniformiser. Par ailleurs, les SI du gouvernement étant intégrés à la passerelle de paiements, le gouvernement peut proposer une expérience utilisateur sans couture.

Au regard du contexte mauritanien et des critères d'évaluation présentés ci-avant, le scénario (2) semble être le plus pertinent pour la Mauritanie. Il offre en effet de très bonnes perspectives pour les administrés en termes de couverture et d'expérience utilisateur tout en assurant au gouvernement un investissement initial réduit ainsi que des efforts de mise en œuvre et d'exploitation limités.

**Les principales activités ont été identifiées afin de mettre en place un modèle opérationnel**



Roadmap de déploiement du modèle opérationnel

**4. Dans un premier temps, il pourrait également être pertinent de mettre en place un modèle phygital**

**Les administrés et les entités publiques n’ont pas encore acquis une maturité digitale suffisante pour adopter pleinement un scénario digitalisé de bout en bout**

La mise en place d’un scénario de digitalisation nécessite quelques adaptations au contexte mauritanien actuel. En effet, l’usage des espèces est encore prépondérant (cf. livrable 1). La population ne connaît pas encore une maturité digitale suffisante pour adopter pleinement les services financiers digitaux et réaliser ses paiements gouvernementaux de manière digitale de bout en bout. De la même manière, les entités publiques fonctionnent encore avec des traitements manuels, bien que quelques applications permettant une gestion informatisée aient été mises en place.

Afin d’assurer le succès de la digitalisation des paiements en permettant une adoption massive du service, il est essentiel de proposer un modèle adapté au contexte actuel, alliant digital et physique.

**Un scénario phygital permet, dans un premier temps, de répondre aux usages et de couvrir un plus large panel d’administrés : en initiant les administrés et les entités publiques au digital, la transition peut se faire en douceur**

Un scénario intermédiaire, appelé « phygital », avant la mise en œuvre d’un modèle digitalisé de bout en bout, permet de réaliser une transition en douceur pour les administrés et les entités publiques. Les administrés peuvent ainsi réaliser leur paiement de services publics au travers de plusieurs types d’interfaces : digitales (web, app mobile, USSD), phygital (GAB, TPE, borne de service) ou physiques (guichet). Ces canaux sont contrôlés par différents acteurs – les entités publiques, le fournisseur de la passerelle de paiement, un fournisseur tiers (fournisseur d’instrument de paiement par exemple) – au même titre que les instruments de paiement centralisés autour d’une passerelle de paiement. L’administré a ainsi la possibilité de régler par espèces ou chèque au travers d’un guichet ou d’une borne de service acceptant ce type de paiement, la digitalisation commençant au niveau de l’agent de l’entité publique, après l’étape du règlement par l’administré. L’administré peut également effectuer son paiement par carte, en se rendant à un GAB ou dans un point de service via un TPE. Dans ce cas,

la digitalisation est également partielle, l'instrument de paiement n'étant pas complètement dématérialisé et l'administré obligé de se déplacer. Enfin, l'administré peut payer de manière totalement digitalisée sans se déplacer en effectuant son paiement à distance par carte bancaire, mobile money ou virement.

<b>Phygital</b>			
Le paiement de services publics se fait au travers de différents types de canaux et instruments de paiement contrôlés par plusieurs acteurs centralisés autour d'un hub de paiement			
<b>1</b>	<b>Interfaces digitales</b>	<ul style="list-style-type: none"> <li>• Web</li> <li>• App mobile</li> <li>• USSD</li> </ul>	Propriété : Entités publiques et / ou fournisseur plateforme de paiement et / ou tiers
	<b>Interfaces phygiales</b>	<ul style="list-style-type: none"> <li>• GAB</li> <li>• TPE</li> <li>• Borne de service</li> </ul>	
	<b>Interfaces physiques</b>	<ul style="list-style-type: none"> <li>• Guichets</li> </ul>	
	<b>Interface unique commande et paiement</b>	Pas systématique (selon le type d'interface)	
<b>2</b>	<b>Inst. paiement digitaux</b>	<ul style="list-style-type: none"> <li>• Mobile money</li> <li>• Virement</li> </ul>	
	<b>Inst. paiement élec.</b>	<ul style="list-style-type: none"> <li>• Carte banc. locale</li> <li>• Carte banc. internat.</li> </ul>	
	<b>Inst. paiement physique</b>	<ul style="list-style-type: none"> <li>• Espèces</li> <li>• Chèques</li> </ul>	
<b>3</b>	<b>SI public intégré avec inst. paiement</b>	Non	
	<b>Contrôle infra. paiement</b>	Fournisseur de la passerelle de paiement	

#### *Caractérisation du modèle « phygital »*

La force de ce modèle intermédiaire est d'apporter une réponse appropriée aux usages et habitudes de la population mauritanienne selon son degré de maturité digitale et financière, tout en initiant la transition vers une digitalisation de bout en bout. Les administrés ont, dans un premier temps, tout un panel d'instruments de paiements à disposition permettant de ne pas être exclus du système. Le gouvernement accompagne ainsi ses administrés vers le paiement entièrement digitalisé.

Dans un projet de digitalisation des paiements gouvernementaux, les entités publiques doivent également réaliser cette transition vers le digital. Le modèle « phygital » permet ainsi de ne pas mettre en œuvre un changement trop brutal. Les agents ont le temps de se familiariser avec le traitement des paiements digitaux et les entités publiques peuvent mieux se préparer aux changements organisationnels impliqués par la digitalisation de bout en bout.

Ce modèle a par exemple été mis en place avec succès en Egypte au travers de la plateforme de paiement Fawry (cf. livrable 1). Les administrés ont la possibilité de réaliser leurs paiements gouvernementaux de manière :

- digitale, via une application, un site web ou un « wallet » mobile
- électronique, avec une carte via un ATM ou un TPE disposé dans un point de service Fawry
- physique, en espèces dans les différents points de service Fawry (bureaux de poste, pharmacie, magasins de détail, etc.)

Le modèle proposé par Fawry a été évolutif puisque la plateforme proposait dans un premier temps le paiement physique ou électronique. Ce n'est que dans un second temps que Fawry a mis en place le paiement digital au travers d'un site web, puis d'une application et enfin via un wallet mobile.

## 7.2. Guide juridique et technique pour la création d'un service digital

### 7.2.1. Préambule

#### 7.2.1.1. Pourquoi ce guide ?

1. Une part importante des échanges entre les usagers et l'administration passe par des procédures administratives qui sont souvent accomplies par le dépôt d'un dossier ou d'une déclaration par un usager auprès d'un service administratif dans un délai déterminé pour acquérir un droit ou se libérer d'une obligation, notamment dans ce dernier cas en réglant une certaine somme. Le terme **téléservice** correspond à la digitalisation d'une procédure administrative.

#### 7.2.1.2. Pourquoi créer un téléservice ?

2. Dans le monde du papier, l'administration demande à l'utilisateur avec qui il échange un niveau de sûreté correspondant à la nature de la situation (appel téléphonique, demande sur papier libre, remplissage de formulaire, envoi simple ou en lettre recommandée avec ou sans accusé de réception, entre autres). Ce niveau de sûreté correspond à une pratique administrative et à un usage du papier satisfaisant depuis des dizaines d'années. Dans le monde numérique au contraire où les risques sont importants, il est obligatoire de mettre en œuvre des mesures de sécurisation qui permettent aux formes dématérialisées de présenter le même niveau de sûreté que si elles s'étaient présentées sur support papier.
3. Les transactions électroniques, c.à.d. les formes dématérialisées des documents et procédures administratives habituelles, doivent être sécurisées. Pour alléger les contraintes sur l'utilisateur, la Loi prévoit que tout service administratif intéressé doit mettre en place un système d'information sécurisé dédié. Ce système d'information est nommé "téléprocédure", "téléservice" ou "profil de l'autorité contractante" dans les marchés publics.

#### 7.2.1.3. A qui s'adresse ce guide ?

4. Ce guide juridique et technique s'adresse :
  - à tous les décideurs et concepteurs de téléservice,
  - aux techniciens qui devront créer le téléservice,
  - aux juristes de l'administration qui devront superviser l'architecture puis la mise en exploitation du téléservice dans le respect de la réglementation.

#### 7.2.1.4. Avertissements

5. Attention, réglementation en cours d'adoption - La réglementation applicative de la Loi sur les transactions électroniques<sup>3</sup> est en cours d'adoption. Les acteurs dans la création d'un téléservice devront vérifier si les textes réglementaires cités ci-après avec le préfixe "projet de ..." ont bien été adoptés. Ils devront faire leur affaire de l'adéquation du texte en appli-

---

<sup>3</sup> Cf. La Loi n° 2018-022 sur les transactions électroniques (ci-après "la Loi").

cation avec les développements de ce guide. Les textes réglementaires en cours sont énumérés dans l'annexe consacrée à la Société de l'Information mauritanienne.

6. Divers textes réglementaires sont en cours d'adoption en application de la Loi n° 2018-022 sur les transactions électroniques (ci-après "la Loi"). Il s'agit de<sup>4</sup> :
  - L'Ordonnance XXX relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives (ci-après "l'Ordonnance"),
  - Le Décret XXX pour l'application de l'ordonnance relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives (ci-après le "décret d'application [de l'Ordonnance]"),
  - Le Décret XXX relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information (ci-après le "Décret d'évaluation"),
  - Le Décret XXX fixant les modalités d'élaboration, d'approbation, de modification et de publication du référentiel général d'interopérabilité (ci-après le "Décret RGS"),
  - Le Décret XXX portant création d'un service à compétence nationale dénommé "Agence nationale de la sécurité des systèmes d'information" (ci-après le "Décret ANSSI"),
  - L'arrêté XXX du Premier ministre pour déclarer la mise en application du RGS.

Les projets de décrets et autres arrêtés actuellement en cours d'élaboration peuvent être provisoirement retenus dans le cadre de ce guide, car ils sont conformes à l'état de l'art et aux normes et standards internationaux.

7. Le Recours à la mutualisation ou aux prestataires et fournisseurs privés - Les lois et règlements encadrant l'administration électronique seront, à moyen terme, nombreux et complexes. Leur mise en application impose au fur et à mesure de leur exécution des points de contrôle et de vérification de conformité. Si une administration désireuse de créer un service électronique ne peut le faire par elle-même ni recourir à la mutualisation des moyens avec d'autres administrations, elle peut faire appel à des équipements et des prestations du secteur privé. Mais les fournisseurs et prestataires du privé devront avoir subi préalablement les mêmes contrôles.

#### **7.2.1.5. Contenu du guide**

8. La partie centrale de ce guide expose comment il est possible de développer un téléservice dans le cadre rigoureux imposé par la réglementation. Quelques annexes complètent le document avec :
  - Un glossaire, car la réglementation en ce domaine n'est pas avare de termes techniques, ce qui n'est pas courant dans les textes juridiques ;

---

<sup>4</sup> IMPORTANT : il est nécessaire de vérifier si les textes réglementaires ont été adoptés et publiés au Journal Officiel.

- Un extrait de la Loi n° 2018-022 relative aux transactions électroniques consacré à l'administration électronique :
- Un canevas pour les "Spécifications Générales et fonctionnelles" du téléservice en création puis en exploitation qui combinent les acteurs, les contraintes juridiques, les normes techniques et les mesures sécuritaires.

## TABLE DES MATIERES

Préambule	58
Pourquoi ce guide ?.....	58
Pourquoi créer un téléservice ?.....	58
A qui s'adresse ce guide ? .....	58
Avertissements.....	58
Contenu du guide.....	59
I- Questions préalables à la création d'un téléservice	64
A- Un procédé hybride papier-électronique peut-il être mis en place ? .....	64
1) Notion de formulaire administratif .....	64
2) Notion de formulaire administratif électronique .....	64
B- Comment le passage du papier à l'électronique est-il possible ? .....	65
C- Que choisir : le dialogue électronique ou le téléservice ? .....	65
D- Peut-on créer un téléservice dans toutes les matières administratives ?.....	66
1) Les services interdits, réservés ou empêchés.....	66
2) Les services libres.....	67
E- Doit-on déjà réfléchir à la réutilisation des données publiques ? .....	68
II- Exigences pesant sur les données	70
A- Organiser l'interopérabilité des données et services.....	70
C- Respecter des données à caractère personnel.....	70
III- Exigences pesant sur la Sécurisation des transactions électroniques	71
A- Comment aborder la sécurité des transactions électroniques.....	71
1) Des exigences de sécurité à respecter et leur niveau à déterminer.....	71
2) Des mesures de sécurité à choisir dans le Règlement Général de Sécurité.....	72
a) Le rôle et les enjeux du RGS .....	72
b) Le régulateur de la sécurité des systèmes d'information .....	73
B- Rechercher les produits et services correspondants .....	73
1) La qualification d'un produit ou d'un prestataire.....	73
2) Les produits et services évalués et certifiés en sécurité – Le référencement.....	74
3) La validation des certificats de signature électronique .....	75

C- Employer des instruments sécuritaires spécifiques.....	76
1) La Signature électronique des autorités administratives .....	76
2) Autres instruments potentiels.....	77
a) Le cachet électronique .....	77
3) Le recommandé électronique et l'horodatage.....	78
IV- Cadre budgétaire de creation du service – Les marchés publics ou les PPP	80
A- Les marchés publics en Mauritanie et les Partenariats Publics-Privés.....	80
1) Des marchés publics aux Partenariats Publics-Privés .....	80
2) Eléments remarquables des PPP .....	81
a) Intérêt des PPP au niveau financier.....	81
b) Intérêt des PPP pour les marchés relatifs aux TIC.....	81
c) Les PPP relatifs aux TIC en Mauritanie .....	82
B- Digitalisation des marchés et des PPP dédiés aux TIC .....	83
1) Dématérialisation de la passation des Marchés Publics .....	83
a) En ce qui concerne les documents du marché.....	83
b) En ce qui concerne la dématérialisation de la procédure.....	84
2) Dématérialisation de la passation des PPP .....	84
a) En ce qui concerne les documents du PPP.....	84
b) En ce qui concerne les étapes de la procédure.....	85
V- Annexes	<b>Erreur ! Signet non défini.</b>
A- Glossaire .....	87
C- Extraits de la Loi n° 2018-022.....	88
D- Elaboration des spécifications générales du service .....	90
0. Préambule – Organisation générale du téléservice .....	90
1) Les acteurs et leur cadre d'intervention.....	90
a) Recensement des acteurs impliqués dans le téléservice .....	90
b) Instruments contractuels et engagements techniques.....	91
2) Le cycle de vie des Données dans le téléservice.....	91
a) Confection initiale des documents .....	91
b) Validation des documents soumis à un téléservice .....	92
c) Préparation et transmission électronique .....	92
d) Journalisation et archivage .....	93
Journalisation .....	93
Archivage électronique.....	93

3) Les moyens de sécurisation du téléservice .....	93
a) Les moyens basiques .....	93
b) Les moyens complémentaires .....	94
c) Sécurisation des terminaux et serveurs .....	94
d) Sécurisation des flux par signature .....	94
Signature numérique et signature électronique .....	95
Type de certificat électronique en support de la signature .....	95

## **7.2.2. I- Questions préalables à la création d'un téléservice**

### **7.2.2.1. A- Un procédé hybride papier-électronique peut-il être mis en place ?**

9. Dans une première étape de digitalisation pour une procédure administrative déterminée, un procédé hybride pourra faire appel conjointement au papier et à l'électronique. Il utilisera en l'occurrence le procédé du formulaire électronique. Ce procédé hybride ne semble pas nécessiter de réglementation spécifique.

#### **7.2.2.1.1. 1) Notion de formulaire administratif**

10. Pour l'instant, le papier reste le support privilégié des déclarations administratives que les particuliers et les entreprises produisent aux services administratifs. Le formulaire administratif est un moyen de respecter un des grands principes du droit public, l'égalité de tous devant les services publics, qui peut se décliner également sous la forme du principe de l'égalité de traitement. Les obligations déclaratives qui forment la base réglementaire des téléservices comme des déclarations papier sont remplies en première étape par le biais d'un document papier identique pour tous les assujettis. Le terme de "formulaire administratif" doit être entendu de façon large puisqu'il peut recouvrir l'ensemble que constituent une grille de demande d'informations, une notice explicative et la liste limitative des pièces justificatives à présenter et quelquefois, un ordre de paiement.
11. Le formulaire est disponible auprès de l'administration créatrice en ses bureaux ou par courrier postal. Internet constitue un moyen récent de diffusion des formulaires. Il s'agit cette fois que l'assujetti ou le déclarant récupère le formulaire en ligne et en réalise une copie papier sur son imprimante avant de le remplir comme il se doit. Cette nouvelle pratique est encouragée par le gouvernement qui y voit comme une marque du développement de l'administration en ligne et le moyen d'une meilleure accessibilité pour le public. Les formulaires dont l'usage est nécessaire pour accomplir une démarche auprès d'une administration ou d'un établissement public administratif de l'Etat doivent être tenus gratuitement à la disposition du public, sous forme numérique, par divers sites d'information administrative du public accessibles sur le réseau Internet.

#### **7.2.2.1.2. 2) Notion de formulaire administratif électronique**

12. L'attachement au support papier n'empêche donc pas les Pouvoirs Publics de préparer la voie au "e-gouvernement". Le passage du formulaire papier transmis par la poste au formulaire électronique transmis via Internet connaîtra deux étapes intermédiaires :
  - L'impression du formulaire papier par l'administré à partir d'un fichier téléchargé sur Internet,
  - La transmission par Internet d'un formulaire à remplir directement à l'écran où Echange de Formulaires Informatisés (EFI).

13. L'aboutissement de la diffusion électronique des formulaires surviendra lorsque le formulaire visible à l'écran pourra être rempli sur le poste informatique et servira à divers services interactifs comme les e-services d'aide à l'accomplissement des formalités administratives, des services personnalisés liés à la démarche (accusé de réception, attribution d'un numéro de dossier, prise de rendez-vous).

#### **7.2.2.2. B- Comment le passage du papier à l'électronique est-il possible ?**

14. Dans un secteur aussi encadré juridiquement que l'administration, le passage du papier à l'électronique n'est pas aussi facile que dans la société civile. C'est la Loi n° 2018-022 relative aux transactions électroniques en Mauritanie qui permet la digitalisation des échanges portant sur des opérations économiques, financières ou se rapportant à toutes autres prestations de services qui s'effectuent en utilisant des technologies numériques<sup>5</sup>.

15. L'article 2 de la Loi n° 2018-022 autorise les transactions électroniques en Mauritanie :

*"Article 2 : La présente loi organise les transactions électroniques et les services par voie électronique en République Islamique de Mauritanie".*

16. Plus loin dans la Loi, tout document papier transmis à l'administration ou issu de celle-ci peut revêtir la forme électronique d'après l'art. 16 :

*Article 16 : L'écrit sous forme électronique est admis pour tous les échanges d'informations, de documents ou d'actes administratifs. Sa transmission peut être effectuée par voie électronique.*

#### **7.2.2.3. C- Que choisir : le dialogue électronique ou le téléservice ?**

17. La Loi précise de quels échanges d'informations il s'agit c'est-à-dire la nature des situations et les types de dialogue électronique potentiels avec l'administration, ainsi :
- Les échanges d'information de toute nature (art. 16) et notamment pour les marchés publics (art. 24), une demande (art. 20), un paiement (art. 22), une information par voie électronique (art. 16), de documents ou d'actes administratifs (art. 16), de pièces justificatives (art. 18),
  - Les formalités administratives (art. 17), les déclarations (art. 19),
  - Les demandes d'information (des usagers) et les réponses (des services administratifs) (art. 18).

---

<sup>5</sup> D'après la définition 20 de l'article de la Loi.

18. Ainsi un usager peut contacter l'administration par mail pour un des types d'échanges cités ci-dessus. Elle pourra lui répondre par le même canal. Mais la forme dématérialisée qui a succédé au document papier doit respecter le même régime juridique, par exemple en identifiant les acteurs, en contrôlant le contenu des documents échangés, en les signant, en garantissant leur date, etc... Toutes ces exigences peuvent être prises en charge par le numérique, à condition d'avoir les compétences nécessaires et des moyens financiers suffisants. C'est pourquoi lorsqu'une formalité est classique et susceptibles d'être accomplies par de nombreux usagers de l'administration (notamment par les assujettis fiscaux), la loi fait obligation à l'administration de créer un vecteur spécifique dédié à cet usage, un téléservice.
19. Appliqué à l'administration électronique, l'art. 2 de la Loi permet de considérer que le dialogue électronique est formé des transactions électroniques directes entre un usager et l'administration et que les services par voie électronique sont constitués de téléservices.
20. La suite des développements de ce guide est consacrée à la création d'un téléservice.

#### **7.2.2.4. D- Peut-on créer un téléservice dans toutes les matières administratives ?**

21. La création d'un téléservice est subordonnée à l'autorisation ou à la possibilité de dématérialiser en la matière.

##### **7.2.2.4.1. 1) Les services interdits, réservés ou empêchés**

22. L'art. 9 de l'Ordonnance stipule que les informations relatives à la défense nationale ne sont pas concernées par le dispositif légal :

*"Article 9 : Les systèmes d'informations traitant d'informations relevant du secret de la défense nationale n'entrent pas dans le champ d'application de la présente ordonnance".*

23. Certains secteurs sont réservés. Ils échappent à ce dispositif légal en possédant leurs propres textes, comme :
  - La Loi n° 2011-003 du 12 janvier 2011 abrogeant et remplaçant la loi n° 96-019 du 19 juin 1996 portant code de l'état civil ;
  - L'Ordonnance n° 2006-031 du 23 août 2006 relative aux instruments de paiement et aux opérations du commerce électroniques en cours de révision<sup>6</sup>.

---

<sup>6</sup> Remarque : Le cadre juridique créé par cette Ordonnance a une portée large car il jette toutes les bases fondamentales favorables à la promotion des TIC au service des échanges économiques et financiers. Le dispositif juridique aborde plusieurs thèmes : preuve électronique,

24. Enfin on peut qualifier de service empêché, le service qui ne peut pas être créé ou exploité pour des raisons techniques ou formelles. Il en va ainsi pour les services qui devraient transmettre des plans ou des montages audio-visuels trop lourds pour pouvoir être transmis sur des vecteurs classiques (Internet par exemple) ou encore, des dossiers qui nécessitent la présence physique de l'auteur au moment du dépôt, etc.

#### 7.2.2.4.2. 2) Les services libres

25. Toutes les matières et les sujets qui ne sont pas visés dans les paragraphes précédents sont libres selon le principe général créé par l'article 2 de la Loi n° 2018-022.
26. En matière administrative, la Loi est complétée par le projet d'Ordonnance qui précise l'application de la Loi au secteur public par opposition au secteur privé.

*"Article 10 : Les dispositions de la présente ordonnance sont applicables en Mauritanie aux administrations de l'Etat et à leurs établissements publics".*

27. Ainsi sauf cas précédents, les actes administratifs et les procédures administratives peuvent être dématérialisés à condition de respecter la sécurisation des pièces électroniques et des transmissions.
28. En effet pour toutes ces hypothèses et modalités de dialogue électronique entre usagers et administration, la Loi 2018-022 envisage la sécurisation des transactions électroniques dans son article 19 :

*Article 19 : Toute autorité administrative mettant en place un système d'information doit obligatoirement prendre les mesures de sécurité nécessaires pour protéger ledit système.*

29. Cette sécurisation est plus large que la simple protection du système contre la cybercriminalité. Elle corrige également les atteintes à la sûreté juridique lorsqu'on passe du papier à l'électronique. La priorité est que l'ordre juridique soit respecté dans la communication entre l'Etat et les citoyens.

---

carte bancaire, virement électronique, commerce électronique et dispositions pénales. Principalement pour le premier thème, cette ordonnance adopte des modifications fondamentales au droit civil mauritanien (code des obligations civiles) en ce sens qu'elle complète dorénavant les règles de preuve dans les relations en instituant le principe de l'admission du support électronique en tant que preuve juridique au même titre et avec la même force juridique probante que l'écrit sur support papier

Source : North Africa backbone Cadre légal et réglementaire V2-1 en version française.

30. Une tentative de catalogue des mesures de sécurisation pour le secteur public peut être établi à partir du texte de la Loi. On y retrouvera :
- L'identification et l'intégrité (art. 77),
  - La sécurité d'accès (largement visée dans la Loi),
  - La confidentialité (art. 85),
  - L'horodatage (art.110).
31. L'identification consiste à établir des mesures permettant de s'assurer de l'identité des personnes ou des entités qui échangent, l'intégrité de garantir que les transactions ne seront pas polluées au cours des échanges et de traitements. La Loi garantit la confidentialité des échanges électroniques ; en cas de difficulté, il faudra recourir à la cryptographie. Enfin, l'horodatage vise à fournir une date qui ne sera pas contestables pour les échanges.

#### **7.2.2.5. E- Doit-on déjà réfléchir à la réutilisation des données publiques ?**

32. Si le droit positif de Mauritanie ne prend pas actuellement en compte la réutilisation des données publiques (qualifiée d'*open data* à l'international), sa mise en œuvre pourrait s'imposer rapidement.
33. A notre époque, les textes juridiques ne sont pas rares qui s'efforcent d'ouvrir informations et données des services administratifs au grand public. L'ouverture des données signifie que leur communication ou leur diffusion se fait au bénéfice de personnes qui n'en sont pas les bénéficiaires naturels. Nombreuses sont en effet les actions de l'administration qui se concluent par la production de documents ou d'information qui ne prennent un sens que lorsqu'ils sont communiqués. Pour que les données publiques soient réutilisées, il faut qu'elles soient communiquées et qu'elles soient exploitables<sup>7</sup>.
34. Aussi les textes fondamentaux sur l'ouverture des données publiques et leur réutilisation se trouvent-ils liés aux textes relatifs à la dématérialisation et au numérique dans le secteur public. La réutilisation des données publiques doit être pensée en amont des traitements techniques, en grande partie par l'interopérabilité, qui est une obligation<sup>8</sup> dans la création d'un téléservice. Le cadre opérationnel de l'Open Data est davantage juridique que technique :

---

<sup>7</sup> Remarque : Dans l'Union Européenne, La Directive 2013/3 du 26 juin 2013 modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public est la base du programme de la région pour le développement de l'Open Data. La directive vise à fixer un ensemble minimal de règles concernant la réutilisation et les moyens pratiques destinés à faciliter la réutilisation de documents existants détenus par des organismes des Etats membres de l'Union européenne. Elle se traduit dans les systèmes d'information publics des membres par une plus grande diffusion d'information et de données publiques.

<sup>8</sup> Cf. INFRA le référentiel général d'interopérabilité (RGI).

- entre ce qui est communicable et ce qui ne l'est pas (Défense Nationale, Propriété Industrielle, données à caractère personnel, motifs pratiques et pertinents des services administratifs) ...
- et les modalités de la communication : transferts électroniques, re-matérialisation sur support papier, droit de Propriété Intellectuelle (notamment Licences Créative Commons), coûts du service ou de la mise à disposition, limitations de la réutilisation.

35. Au total, tout programme d'action organisant le passage au numérique pour une activité ou une branche de l'administration devra, tôt ou tard, mettre en œuvre des données dans une forme et selon un format favorable à la réutilisation desdites données.

### 7.2.3. II- Exigences pesant sur les données

36. Donc, la Loi n° 2018-022 sur les transactions électroniques montre que :
- Les transactions électroniques sont une forme dématérialisée des documents papier. La dématérialisation n'est acquise qu'au moyen de mesures de sécurisation qui permettent aux transactions électroniques de présenter la sûreté juridique requise et qui existait avec le support papier.
  - La possibilité de dématérialiser les documents papier est rendue possible aussi bien pour le secteur privé que pour le secteur public.

#### 7.2.3.1. A- Organiser l'interopérabilité des données et services

37. Le projet d'Ordonnance prévoit que les transactions électroniques doivent être interopérables. Il ne s'agit pas de l'interopérabilité des réseaux, services et équipements de télécommunications, mais d'une interopérabilité applicative comme l'indique l'art. 6 qui met en œuvre un référentiel spécialisé à respecter :

*Article 6 Ord : Un référentiel général d'interopérabilité fixe les règles techniques permettant d'assurer l'interopérabilité des systèmes d'information. Il détermine notamment les répertoires de données, les normes et les standards qui doivent être utilisés par les autorités administratives. Les conditions d'élaboration, d'approbation, de modification et de publication de ce référentiel sont fixées par décret.*

38. L'interopérabilité est indispensable pour que :
- A destination, les données (fichiers, messages) soient lisibles et exploitables par l'humain et quelquefois par la machine,
  - A plus longue échéance, les données puissent être réutilisées (Open Data).
39. Pour prendre un exemple élémentaire, les fichiers de données de format DOC ou PDF seront créés puis lus à destination par de nombreux logiciels disponibles sur le marché.

#### 7.2.3.2. C- Respecter des données à caractère personnel

40. Il s'agit ici de respecter les données à caractère personnel comme le fixe la *Loi n° 2017-20 sur la protection des données à caractère personnel*. Comme tous les acteurs de la Société de l'Information, les services administratifs doivent mettre en œuvre cette protection des données à caractère personnel. L'article 2 de la Loi n° 2018-022 le rappelle :

*"Les dispositions de la présente loi s'appliquent sans préjudice des règles applicables en matière de protection des données à caractère personnel".*

## **7.2.4. III- Exigences pesant sur la Sécurisation des transactions électroniques**

41. Rappel : Les transactions électroniques, c.à.d. les formes dématérialisées des documents et procédures administratives habituelles, doivent être sécurisées pour montrer un niveau de sûreté juridique équivalent à celui du papier. Pour ne pas laisser cette charge aux usagers de l'administration, l'article 19 de la Loi n° 2018-022 pose l'obligation pour le service administratif concerné de créer un téléservice.

Ce système d'information connaît les contraintes suivantes :

- Le service administratif doit établir, sous sa propre responsabilité, les exigences sécuritaires accompagnant la dématérialisation du document ou de la procédure qu'il veut passer à l'électronique, comme le fixe la réglementation.
- Puis il doit mettre en œuvre dans le téléservice les outils sécuritaires nécessaires qui auront été préalablement mis au point par ses agents techniques ou trouvés dans les applications d'un autre service administratif ou encore trouvés chez un fournisseur technique de la société civile, selon les moyens mis à disposition par la réglementation.

### **7.2.4.1. A- Comment aborder la sécurité des transactions électroniques**

#### **7.2.4.1.1. 1) Des exigences de sécurité à respecter et leur niveau à déterminer**

42. Les articles 16 à 24 de la Loi n° 2018-022 regroupés dans un titre intitulé "Section 2 : l'administration électronique" envisagent différentes situations où les transactions électroniques sont échangées entre un usager et l'administration. Tout d'abord, les principes généraux sont énoncés :

- L'écrit électronique est admis ainsi que sa transmission par voie électronique (art. 16),
- Des "systèmes d'information" sécurisés (téléservices) sont mis à la disposition des usagers (art. 19),
- Des accusés de réception électroniques sont employés (art. 20),
- Il n'y a plus de répétition ou de confirmation de l'envoi de documents électroniques de l'utilisateur sur support papier (art. 20).

43. Ensuite, les exigences de sécurisation du téléservice à la charge de l'administration procèdent de la Loi n° 2018-022, puis du projet d'Ordonnance suivi des textes d'applications. L'art. 4 al. 2 du projet de décret d'application de l'ordonnance en fixe le principe :

*"Lorsqu'une autorité administrative met en place un système d'information, elle détermine les fonctions de sécurité nécessaires pour protéger ce système. Pour les fonctions de sécurité traitées par le référentiel général de sécurité, elle fixe le niveau de sécurité requis parmi les niveaux prévus et respecte les règles correspondantes. Un décret précise les modalités d'application du présent alinéa".*

44. L'administration intéressée par la création d'un téléservice, après identification des contraintes sécuritaires à observer pour la création et la mise en exploitation du téléservice, devra, comme le stipule le projet de décret d'application :

- Identifier les besoins de sécurité nécessaires ;
- Déterminer la nature et le degré des mesures de sécurité nécessaires dans les moyens mis à leur disposition par la réglementation (cf. le RGS, ci-dessous).
- Intégrer les mesures de sécurité pertinente dans le téléservice en création.

#### **7.2.4.1.2. 2) Des mesures de sécurité à choisir dans le Règlement Général de Sécurité**

##### **7.2.4.1.3. a) Le rôle et les enjeux du RGS**

45. Les mesures de sécurité susceptibles d'être appliquées dans les transactions électroniques dont l'administration est émettrice ou destinataire sont regroupées dans un référentiel appelé "Référentiel général de sécurité" (RGS), selon l'art. 4 du Décret d'application de l'Ordonnance.

*Article 4 : Un référentiel général de sécurité fixe les règles que doivent respecter les fonctions des systèmes d'information contribuant à la sécurité des informations échangées par voie électronique telles que les fonctions d'identification, de signature électronique, de confidentialité et d'horodatage. Les conditions d'élaboration, d'approbation, de modification et de publication de ce référentiel sont fixées par décret.*

46. Ainsi le RGS explique-t-il comment prendre en charge les fonctions d'identification, de signature électronique, de confidentialité et d'horodatage et quelques autres fonctions de service. La plupart de ces fonctions mettent en œuvre des *certificats électroniques*.

47. Le cycle de vie des certificats électroniques comprend l'enrôlement de l'utilisateur demandeur, la création du certificat, sa distribution, sa révocation, son extinction, ainsi que les intervenants, porteur de certificat, prestataire de confiance, opérateur de confiance, archiveur, horodateur, etc. Le tout est décrit dans un recueil de spécifications appelé *Politique de Certification (PC)*. Le RGS est composé de PC-modèles pour les fonctions de sécurité et de documents annexes.

48. Il existe deux niveaux de sécurité pour les certificats électroniques, selon la pertinence avec laquelle l'identité des demandeurs est contrôlée. D'où des certificats électroniques qu'on peut qualifier de "simples" et des *certificats qualifiés*. Chaque catégorie possède sa PC modèle dans le RGS. Ce schéma en deux niveaux de sécurité est applicable pour tous les types de certificats électroniques.

49. L'administration aura donc déterminé les fonctions de sécurité nécessaires à son téléservice. Elle les documentera en établissant sa propre Politique de certification qui s'inspirera de la PC-modèle correspondante du RGS. A partir de ce moment et dans le respect des documents de spécifications (PC), le téléservice pourra être assemblée en équipements et en logiciels :

- Soit dans l'administration d'origine si elle dispose des moyens techniques nécessaires,
- Soit à partir des fournitures de prestataires commerciaux qui auront été préalablement réputés conformes au RGS par le régulateur.

#### 7.2.4.1.4. b) Le régulateur de la sécurité des systèmes d'information

50. Un projet de décret annonce la présence d'un régulateur dans le domaine des services de domaine appelé "Agence Nationale de la Sécurité des systèmes d'information" (ANSSI). Il indique sur l'ANSSI est chargée d'élaborer, amender et maintenir le RGS.
51. Le RGS est un référentiel technique qui nécessite un instrument juridique pour être reconnu par le Droit et apporter sa caution à la sécurisation des transactions électroniques. C'est pourquoi un autre projet de décret spécialisé précise les conditions d'élaboration, d'approbation, de modification et de publication du RGS -projet de Décret évaluation). Il s'ensuit un arrêté du Premier ministre pour déclarer la mise en application du RGS.
52. Il est nécessaire de se reporter à cet arrêté pour vérifier la version applicable du RGS par son numéro de version, le référentiel étant promis à mise à jour selon l'évolution de l'état de l'art.

#### 7.2.4.2. B- Rechercher les produits et services correspondants

53. L'étude préalable du téléservice à créer s'est achevée sur le dispositif sécuritaire à mettre en œuvre pour ledit service. Il faut désormais rechercher en vue de les assembler les produits et services identifiés. Ces produits et services peuvent exister au sein de l'administration ; ils sont surtout disponibles chez les fournisseurs privés.
54. Les prestataires de services du marché peuvent en effet développer de tels produits et services pour les besoins de la société civile. Mais lorsque la sphère publique est concernée, les produits et services choisis sur le marché doivent être conformes au RGS. Les produits et services doivent subir alors un contrôle de conformité à la réglementation (projet de Décret évaluation) sous le contrôle du régulateur, l'ANSSI, qui s'analyse sur 3 plans de contrôle : la qualification, la certification, la validation.

##### 7.2.4.2.1. 1) La qualification d'un produit ou d'un prestataire

55. L'art. 4 al. 3 du projet de décret d'application traite de la recherche d'un produit de sécurité ou d'un prestataire qualifié. L'alinéa stipule :

*"Les produits de sécurité et les prestataires de services de confiance peuvent obtenir une qualification qui atteste de leur conformité à un niveau de sécurité du référentiel général de sécurité. Un décret précise les conditions de délivrance de cette qualification. Cette délivrance*

*peut, s'agissant des prestataires de services de confiance, être confiée à un organisme privé habilité à cet effet".*

56. La qualification est une attestation délivrée à un produit de sécurité ou un prestataire conforme aux exigences du RGS.
57. La procédure de qualification se déroule sous l'égide de l'ANSSI. La procédure est menée par un auditeur spécialisé (choisi par le candidat et à ses frais) dont l'expertise et le savoir faire ont été préalablement reconnus par l'ANSSI par une accréditation.

#### **7.2.4.2.2. 2) Les produits et services évalués et certifiés en sécurité – Le référencement**

58. Le RGS constitue un pan de la sécurité axé sur les transactions électroniques et leur valeur juridique. Outre le volet transactions électroniques, les produits et services doivent garantir une sécurité technique générale et globale, notamment assurer la disponibilité, l'intégrité ou la confidentialité de l'information traitée face aux menaces de la cyberdélinquance. C'est l'apport du projet de décret relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.
59. Les produits de sécurité et les prestataires de services de confiance qualifiés à un niveau de sécurité peuvent encore faire l'objet d'un référencement par l'Etat. Ils sont alors utilisables par les usagers pour l'ensemble des téléservices pour lesquels ce niveau de sécurité est requis.

*"Article 7 : Les produits de sécurité et les prestataires de services de confiance qualifiés à un niveau de sécurité dans les conditions prévues à l'alinéa trois (3) de l'article 4 peuvent faire en outre l'objet d'un référencement par l'Etat. Ils sont alors utilisables par les usagers pour l'ensemble des téléservices pour lesquels ce niveau de sécurité est requis".*

60. Les agents des autorités administratives chargés du traitement et de l'exploitation des informations recueillies dans le cadre de systèmes d'information utilisent, pour accéder à ces systèmes, des produits de sécurité référencés. Le projet de décret précise les modalités d'application, notamment les conditions de délivrance des produits de sécurité aux agents des autorités administratives.

*"Les agents des autorités administratives chargés du traitement et de l'exploitation des informations recueillies dans le cadre de systèmes d'information utilisent, pour accéder à ces systèmes, des produits de sécurité référencés.*

*Un décret précise les modalités d'application du présent article, notamment les conditions de délivrance des produits de sécurité aux agents des autorités administratives".*

61. Cette procédure est menée par l'ANSSI et aboutit à un certificat de conformité décerné par le Premier ministre, article 8 du projet de décret.

*Article 8 : Le certificat est délivré par le Premier ministre.*

*Il atteste que l'exemplaire du produit ou du système soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Il atteste également que l'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises*

### **7.2.4.2.3. 3) La validation des certificats de signature électronique**

62. Les certificats électroniques des agents sont généralement de type qualifié, surtout si les agents sont des autorités administratives. Le niveau de sécurité est décidé par les concepteurs au moment de l'étude de faisabilité qui mène à la création du téléservice.
63. Les certificats électroniques des agents en vue d'assurer leur identification dans le cadre d'un système d'information font l'objet d'une validation par l'Etat, comme stipulera le projet de Décret.

*Art. 5 : Les certificats électroniques délivrés aux autorités administratives et à leurs agents en vue d'assurer leur identification dans le cadre d'un système d'information font l'objet d'une validation par l'Etat dans des conditions précisées par décret.*

64. En outre, l'ANSSI peut passer des agréments mutuels pour reconnaître en Mauritanie tous types de certificats de sécurités issus d'organismes étrangers homologues.

*"Article 9 : L'Agence nationale de la sécurité des systèmes d'information peut passer, après avis du comité directeur de la certification, des accords de reconnaissance mutuelle avec des organismes étrangers homologues, ayant leur siège en dehors des Etats membres de la Communauté européenne.*

*Ces accords peuvent prévoir que les certificats délivrés par les organismes étrangers cosignataires, dans le cadre de procédures comparables à celle prévue au présent chapitre, sont reconnus comme ayant la même valeur que les certificats délivrés en application du présent décret. La reconnaissance mutuelle des certificats peut être limitée à un niveau d'assurance déterminé".*

### 7.2.4.3. C- Employer des instruments sécuritaires spécifiques

#### 7.2.4.3.1. 1) La Signature électronique des autorités administratives

65. La façon la plus simple de valider au niveau juridique un document, un dossier ou un acte administratif sur papier est de lui apposer une signature manuscrite. L'art. 83 de la Loi définit ce qu'est une signature au regard du Droit : "*La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui en résultent. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte*". Lorsque les actes sont électroniques, à son tour la signature devient électronique. A cet égard, l'art. 83 poursuit : "*Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache*".
66. On remarquera que dans un échange électronique, chacun des acteurs peut être amené, à tour de rôle, à utiliser une signature électronique pour valider ses transactions électroniques. Le procédé de signature électronique est le même pour le secteur public ou la société civile. Cependant un des composants de la signature électronique, le certificat électronique, garantira l'identité dans un cas, d'une autorité administrative et dans l'autre, d'une personne privée.
67. L'art. 85 décide que tout procédé se prétendant "signature électronique" possède cette nature au regard du Droit. C'est pourquoi l'art. 84 pose que dans le domaine juridique, seule la "Signature électronique sécurisée" (SES) peut être apposée à un acte juridique pour assurer sa recevabilité et sa valeur de preuve :

*"Article 85 : Une signature électronique ne peut être déclarée irrecevable au seul motif qu'elle se présente sous forme électronique ; ou qu'elle ne repose pas sur un certificat qualifié ; ou qu'elle n'est pas créée par un dispositif sécurisé de création de signature".*

*Article 84 : Sans préjudice des dispositions en vigueur, une signature électronique sécurisée créée par un dispositif de création de signature sécurisée que le signataire puisse garder sous son contrôle exclusif et dont la vérification repose sur un certificat qualifié est admise comme signature au même titre que la signature autographe<sup>9</sup>".*

68. La SES garantit l'identification du signataire et l'intégrité du document signé. C'est un ensemble technique complexe qui est formé, pour simplifier, d'un logiciel de création de signature (qualifié de "dispositif") et d'un certificat électronique (le "procédé d'identification").

---

<sup>9</sup> En ce qui concerne la "signature autographe" de l'article 84, on comprendra qu'il s'agit d'une signature "manuscrite".

L'art. 82 de la Loi reconnaît que les administrations peuvent employer des signatures électroniques, tandis que l'art. 3 du projet de décret d'application stipulera qu'elle doit être conforme au RGS :

*"Article 3 : Les actes des autorités administratives peuvent faire l'objet d'une signature électronique. Celle-ci n'est valablement apposée que par l'usage d'un procédé, conforme aux règles du référentiel général de sécurité mentionné à l'alinéa un (1) de l'article 4, qui permette l'identification du signataire, garantisse le lien de la signature avec l'acte auquel elle s'attache et assure l'intégrité de cet acte".*

69. Dans le contexte d'un téléservice, c'est l'administration promotrice qui déterminera la signature électronique à utiliser par l'utilisateur. L'utilisateur pourra employer, à ses frais, n'importe quels produits du marché (dispositif de création et un certificat électronique) qui auront fait préalablement l'objet d'une qualification auprès de l'ANSSI.
70. Note : si l'administration signe électroniquement ses actes, ses usagers peuvent l'avoir saisi préalablement par une requête ou avoir expédié un dossier sur lesquels sera également apposé une signature électronique. Dans ce cas, d'autres types de signature seront peut-être utilisés par l'utilisateur, surtout s'il est installé à l'étranger, comme des Signatures électroniques avancées ou des Signatures électroniques qualifiées<sup>10</sup>, ou encore des cachets électroniques.

#### **7.2.4.3.2. 2) Autres instruments potentiels**

##### **7.2.4.3.2.1. a) Le cachet électronique**

71. Un téléservice pourrait recevoir des transactions électroniques munies d'un cachet électronique en lieu et place de la signature électronique attendue.
72. La justification du "cachet électronique" est la suivante. Les personnes morales sont généralement considérées dans les systèmes juridiques comme une "fiction juridique" et par conséquent sont incapables de produire par elle-même un document ou un acte juridique. Elles ne peuvent pas non plus signer et attribuer à leur signature tous les effets juridiques

---

<sup>10</sup> REMARQUE : En Europe depuis le Règlement (UE) n° 910/2014 du Parlement Européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, l'intégration de la *signature qualifiée* conforte une pratique et une analyse juridique qui s'étaient installées depuis plusieurs années aussi bien au niveau européen qu'en France. La SE qualifiée est la seule à porter les effets juridiques de la signature électronique. Elle bénéficie du support d'un certificat électronique "qualifié".

A noter également que l'OHADA prévoit dans l'art. 83 de son AUDCG l'utilisation de signature électronique de type "qualifié" pour les questions juridiques.

attachées à cet instrument. D'où le concept de cachet électronique qui doit servir à prouver qu'un document électronique a été délivré par une personne morale en garantissant l'origine et l'intégrité du document. Dans les pays membres de l'Union Européenne, les seuls effets juridiques pertinents appartiennent évidemment au cachet électronique "qualifié".

73. A défaut de cachet électronique dans le droit positif<sup>11</sup>, on proposera d'appliquer la signature électronique qualifiée du chef d'entreprise, à condition d'être en mesure de démontrer que le signataire est réellement le chef d'entreprise ou son mandataire (dans le certificat électronique ou par tout autre moyen).

#### 7.2.4.3.3. 3) Le recommandé électronique et l'horodatage

74. Signer électroniquement une déclaration qu'un usager dépose sur un téléservice ne garantit pas que cette dernière arrive bien à destination et dans les délais impartis. Dans le monde du papier, on fait appel à un envoi recommandé (postal) avec ou sans accusé de réception. La possibilité existe dans la sphère du numérique ; elle est mentionnée dans l'art. 11 de la Loi 2018-022 :

*"Article 11 : Le message signé électroniquement, sur la base d'un certificat électronique conforme aux dispositions légales et réglementaires, et dont l'heure et la date sont certifiées par le prestataire, constitue un envoi recommandé."*

75. La Loi 2018-022 décrit cette procédure particulière dans le cadre de l'administration électronique<sup>12</sup> :
- Délivrance obligatoire par l'administration en cas de demande, déclaration, paiement ou une information par voie électronique (art. 20).
  - Contenu de l'AR : date de réception de la demande, service saisi et date à laquelle cette demande sera acceptée ou rejetée. Le cas échéant, il doit mentionner le délai de réponse (art.20).
  - Procédure de l'AR : un message électronique, signé et avec une certification du temps garanti par le prestataire. Des précisions pourront être apportées par le RGS.
76. Un des éléments primordiaux de cette procédure est une garantie dans la datation du message, ce qui conduit à trois remarques :

---

<sup>11</sup> REMARQUE : vérifier si le cachet électronique est prévu par le RGS.

<sup>12</sup> ATTENTION : l'accusé de réception existe également dans le Commerce électronique avec des modalités d'emploi différentes (art. 48 à 58 de la Loi).

- Les procédures administratives sont souvent à accomplir dans un délai déterminé, avec quelquefois un paiement à effectuer.

- Les délais de recours sont suspendus si l'accusé de réception n'a pas été délivré ou est incorrect :

*"Article 21 : Les délais de recours résultant des prescriptions de l'article précédent ne sont pas opposables à l'utilisateur lorsque l'accusé de réception ne lui a pas été transmis ou ne comporte pas les indications mentionnées à l'article précédent".*

- Certaines transactions, notamment venant de l'étranger<sup>13</sup>, peuvent employer soit un système de recommandé, soit un système de datation technique appelé "horodatage"<sup>14</sup> <sup>15</sup>

---

<sup>13</sup> REMARQUE : Dans l'UE, le recommandé électronique s'entend d'un service qui permet de transmettre des données par voie électronique, qui fournit des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi ou de leur réception, et qui protège les données transmises contre les risques de perte, de vol, d'altération ou de toute modification non autorisée (art. 3.28 définitions). Les données envoyées ou reçues sont alors recevables comme preuves en justice en ce qui concerne l'intégrité des données et l'exactitude de la date et l'heure à laquelle les données ont été envoyées ou reçues par un destinataire déterminé (art. 35 du Règlement).

<sup>14</sup> REMARQUE : l'horodatage met en œuvre des certificats électroniques spécialisés appelés "jetons d'horodatage" émis par des prestataires spécialisés dits "autorités d'horodatage". Le référentiel européen (le Règlement précité) des services de confiance connaît ce système.

<sup>15</sup> REMARQUE : vérifier si le recommandé électronique et l'horodatage sont prévus par le RGS

## **7.2.5. IV- Cadre budgétaire de creation du service – Les marchés publics ou les PPP**

### **7.2.5.1. A- Les marchés publics en Mauritanie et les Partenariats Publics-Privés**

#### **7.2.5.1.1. 1) Des marchés publics aux Partenariats Publics-Privés**

77. La création et la mise en exploitation d'un téléservice suppose l'assemblage d'un nombre, qui peut être élevé, de services et d'équipements techniques prenant en charge la dématérialisation des procédures administratives écrites sur papier et la sécurisation des flux électroniques qui l'accompagne. Si l'administration intéressée à la création et à la mise en exploitation du téléservice ne dispose pas de toutes les capacités techniques et financières, elle fera classiquement appel aux marchés publics pour obtenir ce qu'elle recherche. Il sera alors fait application de la Loi n° 2010-044 du 22 juillet 2010 portant Code de Marchés Publics et du Décret n° 2017-126 du 2 novembre 2017 abrogeant et remplaçant les dispositions des décrets d'application de la loi 2010-044 du 22 juillet 2010 portant Code des marchés publics. Le marché public se présente comme un "*contrat écrit, conclu à titre onéreux, (...), par lequel un entrepreneur, un fournisseur, ou un prestataire de services s'engage envers l'une des personnes morales publiques (...), soit à réaliser des travaux, soit à fournir des biens ou des services moyennant un prix*" (art. Premier du Code).
78. Cependant l'objectif recherché, le téléservice, peut supposer une large prise en compte du service rendu et de son environnement qui déborde l'aspect technique. L'attributaire du marché peut se voir confié une mission globale relative au financement d'investissements immatériels, d'ouvrages ou d'équipements nécessaires au service, à la construction ou à la transformation des ouvrages ou équipements, ainsi qu'à leur entretien, leur maintenance, leur exploitation ou leur gestion, et, le cas échéant, à d'autres prestations de services concourant à l'exercice, par la personne publique, de la mission de service public dont elle est chargée.
79. Ces contraintes étaient anciennement prises en charge par une catégorie d'achat public dite "marché de partenariat". Suite à certains exemples étrangers (comme la "Project Finance Initiative" lancée au Royaume-Uni en 1992), cette catégorie a évolué en une forme de contrat global prenant en charge toutes les facettes de l'opération, le partenariat public-privé (PPP). Les PPP permettent de sortir des limites inhérentes aux deux formes classiques de contrats administratifs : le marché public et la délégation de service public. Les contrats de partenariat autorisent une plus grande souplesse de gestion pour la personne publique, tout en assurant qu'elle reste en charge de la gestion du service public.
80. En Mauritanie, l'encadrement juridique des PPP procède des textes suivants :
- Loi n° 2017-006 du 01 février 2017 relative au Partenariat Public-Privé (PPP).
  - Décret d'application n° 2017-126 du 02 novembre 2017 abrogeant et remplaçant les dispositions des décrets d'application de la loi n° 2010-044 du 22 juillet 2010 portant Code des marchés publics.
  - **Arrêté n° 828-2016 PM du 31 août 2016 portant sur la création du Comité Interministériel du Développement des PPP.**
  - Arrêté n° 850-2016 MEF du 8 sept. 2016 portant sur la création du Comité Technique d'Appui au Développement des PPP.
  - Arrêté n° 0915/MEF du 3 novembre 2017 fixe les seuils des procédures applicables aux PPP.

81. L'article n° 1 de la loi n° 2017-006 définit clairement le concept de PPP en exposant que "le contrat administratif de partenariat public-privé, conclu entre l'Autorité Contractante et une personne morale de droit privé ou de droit public (opérateur économique), portant sur une mission globale relative à un ouvrage d'intérêt général ou d'utilité publique et/ou portant sur l'exploitation d'un service public".

#### **7.2.5.1.2. 2) Eléments remarquables des PPP**

82. Les sources d'information sur les PPP ne sont pas rares ni en Mauritanie<sup>16</sup> ni à l'étranger.

##### **7.2.5.1.2.1. a) Intérêt des PPP au niveau financier**

83. Les PPP permettent l'association, de manière durable, d'un ou plusieurs entrepreneurs privés à la construction, à l'entretien et/ou à la gestion d'un ouvrage public. Le marché de partenariat implique un financement principalement privé.
84. Le marché de partenariat est un contrat à paiement public différé. Le cocontractant privé est rémunéré sous forme de loyers à compter de la mise à disposition des ouvrages construits. Cette rémunération est liée à des critères de performance fixés par le contrat pour chacune de ses phases.
85. La passation d'un marché de partenariat doit être autorisée par l'autorité compétente (ministres chargés du budget et de l'économie pour les marchés passés par l'État et autres organismes de suivi).

##### **7.2.5.1.3. b) Intérêt des PPP pour les marchés relatifs aux TIC**

86. Ce guide s'intéresse à l'emploi d'un PPP pour le financement d'un téléservice dans l'administration mauritanienne. Sur ce plan, il semble que l'emploi d'un PPP soit plus efficace dans le domaine des technologies de l'information et de la communication que pour

---

<sup>16</sup> Voir le site dédié d'URL : [www.ppp.gov.mr](http://www.ppp.gov.mr) et notamment le "Guide opérationnel des PPP en Mauritanie" par la Cellule d'appui aux PPP, Ministère de l'Économie et des Finances.

d'autres matières<sup>17</sup>.

87. Selon la Banque Mondiale (BM), les innovations dans le domaine des technologies de l'information et de la communication (TIC) ainsi qu'une hausse de la demande du marché ont eu des conséquences importantes pour les services de télécommunications publics et pour l'infrastructure des TIC, et notamment une tendance à la déréglementation et la libéralisation des marchés des télécommunications<sup>18</sup>.
88. En outre, le programme spécialisé de la BM, InfoDev, présente une carte des connaissances et un manuel (juin 2009) conçus pour fournir aux décideurs, au personnel des agences de développement, aux partenaires du secteur privé et à d'autres praticiens clés des conseils sur les politiques, programmes, services et instruments susceptibles de faciliter l'engagement du secteur privé dans des domaines traditionnellement considérés comme étant uniquement ceux du gouvernement<sup>19</sup>.

#### 7.2.5.1.3.1. c) Les PPP relatifs aux TIC en Mauritanie

89. Compte-tenu de son intérêt, un PPP est plus avantageux pour la création d'un téléservice dans une administration mauritanienne qu'un classique marché public. La Loi n° 2017-06 va d'ailleurs dans ce sens, puisque son article 3 "Champ d'application de la Loi PPP" déclare :

*"Cette loi s'applique à tous les secteurs de la vie économique et sociale en Mauritanie sous réserve des dispositions applicables à la Zone Franche de Nouadhibou, ainsi qu'aux autorisations, conventions, licences et contrats déjà réglementés dans les secteurs suivants :*

- *Le secteur minier ;*
- *Le secteur des hydrocarbures bruts ;*
- *Le secteur des télécommunications <sup>20</sup>;*

---

<sup>17</sup> Voir comme exemple, le Rapport spécial "Les partenariats public-privé dans l'UE : de multiples insuffisances et des avantages limités", Cour des comptes européennes, rapport n°9, 2018.

URL : [https://www.eca.europa.eu/Lists/ECADocuments/SR18\\_09/SR\\_PPP\\_FR.pdf](https://www.eca.europa.eu/Lists/ECADocuments/SR18_09/SR_PPP_FR.pdf)

<sup>18</sup> Dans cette section du portail internet du Centre de ressources (BM) des PPP dans le secteur des infrastructures (PPPLRC), on peut trouver des ressources utiles à la compréhension, l'évaluation et la mise en œuvre de la réforme du secteur des télécommunications et des TIC d'un pays.

URL : <https://ppp.worldbank.org/public-private-partnership/fran%C3%A7ais/ppps-par-secteur/les-ppp-dans-le-domaine-de-la-t%C3%A9l%C3%A9communication-et-des-technologies-de-l%E2%80%99i>

<sup>19</sup> Voir : <https://www.infodev.org/articles/public-private-partnerships-ppps-e-government-knowledge-map-0>

<sup>20</sup> Dans cette note, c'est nous qui avons souligné les passages notables des textes.

qui restent régis, pour ce qui est de la Zone Franche par sa législation propre et pour ce qui est des secteurs précités par leurs législations sectorielles.

*Les dispositions de la présente loi sont d'ordre public, sauf pour les Contrats de PPP transfrontaliers et les Contrats de PPP passés en application d'accords de financement ou de traités internationaux qui sont soumis aux dispositions de la présente loi, dans la mesure où leurs dispositions ne sont pas contraires à celles des accords et traités internationaux.*

#### **7.2.5.2. B- Digitalisation des marchés et des PPP dédiés aux TIC**

90. Dans l'optique du développement de la Société de l'information en Mauritanie et notamment, de l'administration électronique, il importe de regarder comment la mise en œuvre des deux modes de commande publique peut être dématérialisée.

##### **7.2.5.2.1. 1) Dématérialisation de la passation des Marchés Publics**

###### **7.2.5.2.1.1. a) En ce qui concerne les documents du marché**

91. Les réponses sur le contenu de la dématérialisation dans la procédure des marchés se trouvent dans le Code des marchés publics (CMP) qui en définit le terme dans son article premier : *"Dématérialisation : la création, l'échange, l'envoi, la réception ou la conservation d'informations ou de documents par des moyens électroniques ou optiques, ou des moyens de messagerie électronique ; comparables, notamment, mais non exclusivement, l'échange de données informatisées"*.
92. La passation d'un marché public est une procédure complexe où plusieurs flux de données peuvent être échangés entre une administration dite "autorité contractante" et un acteur économique appelé "candidat. C'est ainsi que l'art. 35 Champ d'application du CMP pose le principe général de la dématérialisation de la procédure :

*"Article 35 : Les échanges d'informations intervenant en application de la présente loi peuvent faire l'objet d'une transmission par voie électronique dans les conditions définies aux articles 36 et 37 ci-dessous"*.

93. Comme souvent, il n'est pas toujours rappelé à chaque détour de texte que et le support papier et la forme électronique sont possibles<sup>21</sup>. L'article 36 précise ce point : *"Les dispositions de la présente loi qui font référence à des écrits ne font pas obstacle au remplacement de ceux-ci par un support ou un échange électronique"*. Ainsi les échanges d'information sont-ils principalement constitués :
- Pour l'autorité contractante : de documents d'appel d'offres et de consultation. Ces documents sont mis à la disposition des candidats par voie électronique, sauf possibilité pour les candidats de demander un envoi par la poste.

---

<sup>21</sup> Rappel : l'équivalence entre l'écrit sur support papier et l'écrit sous forme électronique est instaurée par l'article 77 de la Loi n° 2018-022 sur les transactions électroniques.

- Pour les candidats : de candidatures et d'offres qui peuvent être transmis par la voie électronique sauf disposition contraire des documents de consultation.

94. Au niveau économique, les marchés publics sont un secteur assez sensible économiquement, ce qui occasionne les garanties formulées par l'art. 37 :

*"Art. 37 : Les outils utilisés pour communiquer par des moyens électroniques, ainsi que leurs caractéristiques techniques, doivent avoir un caractère non discriminatoire, être couramment à la disposition du public et compatibles avec les technologies d'information et de communication généralement utilisées.*

#### 7.2.5.2.1.2. b) En ce qui concerne la dématérialisation de la procédure

95. S'agissant des mesures de publicité et selon l'article 15 du Code, les autorités contractantes sont tenues d'élaborer au début de chaque année des plans prévisionnels annuels de passation des marchés publics renfermant toutes les acquisitions de biens et services sur la base de leur programme d'activité. Les autorités contractantes en assurent la publicité dans un journal à diffusion nationale ainsi que sur un site électronique commun dont l'accès doit être forcément gratuit au plus tard trente jours calendaires avant la date de la première passation mentionnée dans le plan prévisionnel.
96. S'agissant de l'entrée en vigueur du marché, l'article 47 indique : "Le marché entre en vigueur dès sa notification... Dans les quinze (15) jours calendaires de l'entrée en vigueur du marché, un avis d'attribution définitive est publié dans le bulletin Officiel des Marchés Publics, ou par voie électronique ou tout autre moyen de publication".
97. En cas de différends entre les parties et d'après l'art. 53, un recours peut être exercé devant la Commission de règlement des différends soit par lettre recommandée avec accusé de réception, soit par tout moyen de communication électronique selon les modalités du Code. La saisine de la commission de règlement des différends entraîne une suspension immédiate de la procédure de passation. L'avis de suspension de la procédure doit être publié par la Commission deux jours ouvrables après sa saisine dans un quotidien local de large diffusion, sur un site électronique commun et gratuit et dans la première publication du Bulletin officiel des marchés publics.

#### 7.2.5.2.2. 2) Dématérialisation de la passation des PPP

##### 7.2.5.2.2.1. a) En ce qui concerne les documents du PPP

98. La dématérialisation des PPP, renforcée par la sécurisation des transactions électroniques, est actée par le Décret 2017-126 :

*"Art. 29 : Dans toutes les procédures de passation des contrats de partenariat public privé, les communications et les échanges d'informations effectués (...) peuvent être effectués par la voie électronique... Les communications, les échanges et le stockage*

*d'informations se font dans des conditions permettant de respecter l'intégrité des données et la confidentialité des candidatures, des offres et des demandes de participation jusqu'à l'expiration du délai prévu pour leur présentation".*

99. Selon l'art. 27, les informations et pièces nécessaires sont largement ouvertes aux formes électroniques :

*"Chaque candidat est tenu de remettre à l'appui de sa candidature les pièces suivantes :1) Le nom, le prénom, la qualité et le domicile du candidat ainsi que les numéros de téléphone, de fax et de l'adresse électronique, et s'il s'agit d'une société, son nom, sa raison sociale, sa forme juridique, son capital social, l'adresse de son siège social, ainsi que la qualité du candidat pour laquelle il agit et les pouvoirs qui lui sont conférés..."*

#### 7.2.5.2.2.2. b) En ce qui concerne les étapes de la procédure

100. La procédure dématérialisée et sécurisée se déroule selon les principes suivants (art. 24 et 29 du Décret) :

- Publicité de l'appel d'offres pour un PPP, l'article 25 prévoit que l'avis sera "publié sur le site électronique de l'autorité contractante et dans au moins un journal à large diffusion nationale". D'après l'art. 24, l'avis d'appel d'offres comprend nécessairement les mentions suivantes l'adresse électronique du site utilisé pour la publication de l'avis<sup>22</sup>. Quant aux documents de l'appel d'offres ou de consultation, ils peuvent être transmis aux candidats par voie électronique ou par voie postale.
- Mode de transmission : Il est indiqué dans l'avis d'appel d'offres ou, en l'absence d'un tel avis, dans les documents de la consultation. Si l'utilisation du site de l'appel d'offres est libre et gratuite, les frais d'accès au réseau restent à la charge du candidat.
- Pour chaque étape de la procédure, les candidats et soumissionnaires appliquent le même mode de transmission à l'ensemble des documents qu'ils transmettent à l'autorité contractante.
- Attribution du PPP (art. 55) : avis d'attribution publié au Bulletin Officiel des Marchés publics, ou par voie électronique ou tout autre moyen de publication.

101. Attention à l'art. 25 du Code sur l'obligation de publicité, les marchés publics, dont le montant est supérieur à un arrêté du Premier ministre, doivent obligatoirement faire l'objet d'un avis d'appel d'offres porté à la connaissance du public par une insertion faite dans le Bulletin Officiel des Marchés Publics ou toute publication nationale ainsi que sous mode électronique. Et l'art. 25 de conclure : "*L'absence de publication de l'avis d'appel d'offres*

---

<sup>22</sup> Il s'agit de l'URL du site.

*lorsqu'il est requis est sanctionnée par la nullité de toute la procédure".*

## 7.2.6. A- Glossaire

- Certificat électronique : un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire ;
- Certificat électronique qualifié : en plus de sa qualité de document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire, il répond en outre aux exigences définies par la présente loi ;
- Commerce électronique : activité économique par laquelle une personne, physique ou morale, propose ou assure à distance et par voie électronique, la fourniture de biens et/ou la prestation de services ;
- Dématérialisation" s'entend comme la substitution d'une forme électronique à un document juridique sur papier. Différemment, passer un document papier sur un scanner est une "numérisation".
- Dispositif de création de signature électronique : un matériel ou un logiciel permettant la création d'une signature électronique ;
- Dispositif de vérification de signature électronique : un matériel ou logiciel permettant la vérification de signature électronique ;
- Dispositif sécurisé de création de signature électronique : un dispositif qui satisfait aux exigences définies par la présente loi ;
- Document électronique : ensemble de données enregistrées ou mises en mémoire sur quelque support que ce soit par un système informatique ou un dispositif semblable et qui peuvent être lues ou perçues par une personne ou par un tel système ou dispositif. Sont également visés, tout affichage et toute sortie imprimée ou tout autre traitement de ces données ;
- Fournisseur de service : toute personne physique ou morale utilisant des supports, systèmes ou réseaux des Technologies de l'Information et la Communication, pour offrir des services ;
- Prestataire de services de certification électronique : toute personne qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique ;
- Prestataire de services de confiance : toute personne offrant des services tendant à la mise en œuvre de fonctions qui contribuent à la sécurité des informations échangées par voie électronique;
- Qualification des prestataires de services de certification électronique : l'acte par lequel un tiers, en l'espèce l'Autorité de Certification, atteste qu'un prestataire de services de certification électronique fournit des prestations conformes à des exigences particulières de qualité ;
- Signataire : toute personne qui détient un dispositif de création de signature et qui agit soit pour son propre compte, soit pour celui d'une personne physique ou morale qu'elle représente ;
- Signature électronique (SE) : une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de procédé d'identification ;
- Signature électronique sécurisée (SES) : une SE créée par un dispositif de création de signature sécurisée et dont la vérification repose sur un certificat qualifié ;
- Système d'information : tout ensemble de moyens destinés à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives ;
- Téléservice », tout système d'information permettant aux usagers de procéder par voie électronique à des démarches ou formalités administratives.
- Transactions électroniques : échanges électroniques portant sur des opérations économiques, financières ou se rapportant à toutes autres prestations de services qui s'effectuent en utilisant des technologies numériques ;

## 7.2.7. C- Extraits de la Loi n° 2018-022

### SECTION 2 : L'ADMINISTRATION ELECTRONIQUE

**Article 16** : L'écrit sous forme électronique est admis pour tous les échanges d'informations, de documents ou d'actes administratifs. Sa transmission peut être effectuée par voie électronique.

A cette fin, chaque administration communique les coordonnées électroniques permettant d'entrer en contact avec elle.

En outre, toute personne physique ou morale qui souhaite être contactée par l'Administration par courrier électronique, lui communique les coordonnées nécessaires pour ce faire. Elle veille à consulter régulièrement sa messagerie électronique et à signaler à l'administration tout changement de coordonnées.

**Article 17** : Lorsqu'une formalité prévue par les dispositions de l'article 5 de la présente loi est exigée au cours d'une procédure administrative, l'Administration recourt aux équivalents fonctionnels reconnus par la présente loi, à moins que l'application de règles plus strictes se justifie, eu égard à la particularité de la procédure et des documents concernés.

**Article 18** : Une autorité administrative peut répondre par voie électronique à toute demande d'information qui lui a été adressée par cette voie par un usager ou par une autre autorité administrative.

Lorsqu'il est exigé qu'une pièce justificative soit jointe à l'appui d'une demande ou d'une déclaration adressée à l'Administration, le demandeur est dispensé de fournir cette pièce par voie électronique lorsque l'Administration peut se la procurer directement auprès de l'autorité administrative concernée, à condition que l'intéressé l'ait préalablement accepté de manière expresse.

Dans ce cas, la fourniture du document est remplacée par une déclaration sur l'honneur du demandeur, qui a la possibilité de vérifier, par voie électronique, les informations prises en compte par l'Administration.

**Article 19** : Toute autorité administrative mettant en place un système d'information doit obligatoirement prendre les mesures de sécurité nécessaires pour protéger ledit système.

**Article 20** : Lorsqu'un usager a transmis par voie électronique à une autorité administrative une demande, une déclaration, un paiement ou une information par voie électronique, il doit recevoir en retour un accusé de réception.

L'accusé de réception doit préciser la date de réception de la demande, le service saisi et la date à laquelle cette demande sera acceptée ou rejetée. Le cas échéant, il doit mentionner le délai de réponse.

L'autorité administrative doit traiter le dossier sans exiger de l'usager la confirmation ou la répétition de l'envoi de sa correspondance sous une autre forme.

**Article 21** : Les délais de recours résultant des prescriptions de l'article précédent ne sont pas opposables à l'usager lorsque l'accusé de réception ne lui a pas été transmis ou ne comporte pas les indications mentionnées à l'article précédent.

**Article 22** : Lorsqu'un paiement est exigé du demandeur au cours d'une procédure administrative, notamment pour l'obtention d'une attestation ou d'un document officiel, ce paiement peut avoir lieu par voie électronique, suivant les conditions et les modalités définies par l'Administration.

**Article 23** : L'autorité administrative n'est pas tenue d'accuser réception des envois abusifs, notamment par leur nombre, leur caractère répétitif ou systématique.

**Article 24** : Les échanges d'informations intervenant en application du code des marchés publics peuvent faire l'objet d'une transmission par voie électronique.

Les modalités d'application du présent article sont fixées par des dispositions réglementaires.

## 7.2.8. D- Elaboration des spécifications générales du service

Le premier stade de l'étude de création d'un téléservice correspond à une étude de faisabilité au cours de laquelle on dressera les spécifications générales du service. Ces spécifications pourront comporter les éléments déclaratifs qui suivent.

### 7.2.8.1. 0. Préambule – Organisation générale du téléservice

Le téléservice contient des Données, prises isolément ou assemblées en messages, fichiers, classeur ou dossier, utilisées dans et par le secteur public et qui sont soumises à des exigences juridiques variées :

- Les contraintes générales issues de l'*Ordonnance ... relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives* et notamment les exigences de sécurité et d'interopérabilité.
- Les exigences spécifiques posées par des textes réglementaires spécifiques selon la nature des Données,
- Les contraintes du droit commun du fait du caractère lacunaire des sources précédentes.

Certaines conformités légales et réglementaires spéciales doivent être assurées, comme :

- Protection des données personnelles : tout téléservice respecte les dispositions de la *loi n° 2017-20 sur la protection des données à caractère personnel* et les règles de sécurité et d'interopérabilité de l'*Ordonnance... relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives*.
- Cryptologie : Les moyens de cryptologie utilisés en l'état (c'est-à-dire appliqués aux garanties d'identification et d'intégrité) ne nécessitent pas l'accomplissement de formalités particulières.

Le présent téléservice repose sur une architecture composée de plusieurs types d'applications, notamment :

- La gestion des Données déposés ou numérisés, échangés ou transmis,
- La sécurisation des Données, notamment par signature numérique ou électronique, par horodatage,
- La transmission sécurisée des flux électroniques de données,
- L'archivage des Objets et des flux, émis ou reçus, ainsi que des preuves de traitement, garanti par un coffre numérique.

### 7.2.8.2. 1) Les acteurs et leur cadre d'intervention

#### 7.2.8.2.1. a) Recensement des acteurs impliqués dans le téléservice

Les étapes du cycle de vie des Données dans le téléservice voient intervenir les acteurs qui suivent :

- L'émetteur : l'entité juridique qui dépose un document, sous forme électronique ou sur support papier, ou un ensemble de données pour bénéficier d'un ou plusieurs traitements offerts par un

téléservice avant mise à disposition ou transmission à un ou plusieurs Destinataires.

- Le destinataire : l'entité juridique qui reçoit un ensemble de données électroniques ou pour lequel cet ensemble est mis à disposition par un téléservice, après des traitements opérés pour le compte de l'Emetteur.
- L'autorité de certification : le service utilise plusieurs types de certificats électroniques
- L'autorité d'horodatage : le service est susceptible de jouer le rôle de tiers horodateur, sauf pour les services expressément spécifiés dans cette PS qui nécessitent une Autorité d'Horodatage externe.
- Autres...

### **7.2.8.2.2.** b) Instruments contractuels et engagements techniques

Les aspects opérationnels du téléservice sont encadrés par des instruments contractuels et réglementaires, ainsi :

- Le contrat de prestation de service avec le Tiers de transmission,
- Le contrat de prestation de service de certification électronique,
- Le contrat de prestation de service d'horodatage, s'il y a lieu,
- Le contrat de prestation de service d'archivage, s'il y a lieu,

Les engagements techniques et fonctionnels du prestataire sont décrits dans plusieurs recueils de spécifications, notamment :

- Les Politiques de Certification : la PC est un document qui réunit des règles, identifié par un nom, définissant le type d'application auxquelles un certificat est adapté ou dédié ainsi que les différentes étapes et modalités de son cycle de vie. Le téléservice fait référence à N politiques de certification qui sont : ....
- La Politique d'Archivage : c'est le document qui définira les exigences minimales, en termes juridiques, fonctionnels, opérationnels, techniques et de sécurité, applicables aux actions visant à identifier, recueillir, classer, conserver, communiquer et restituer des documents électroniques, pour la durée nécessaire à la satisfaction des obligations légales ou pour des besoins d'informations ou à des fins patrimoniales.
- La Politique d'Horodatage : c'est le document qui rassemble l'ensemble des règles définissant les exigences auxquelles un tiers archiveur se conforme pour la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'une contremarque de temps à une communauté particulière et/ou une classe d'application avec des exigences de sécurité communes.
- Le Plan de Reprise d'Activité ou le Plan de Continuité d'Activité (PRA / PCA)
- La documentation technique sur l'initialisation et le fonctionnement du Service.

### **7.2.8.3. 2) Le cycle de vie des Données dans le téléservice**

#### **7.2.8.3.1.** a) Confection initiale des documents

Ces dispositions concernent les documents pris en charge par le téléservice, soit sous une forme électronique, soit sur support papier et qui seront soumis à dématérialisation. Tout Objet numérique déposé ou transmis à un téléservice est susceptible, selon son type et sa nature juridique, d'être composé comme suit :

- Un document principal,
- Une ou plusieurs pièces attachées

Sauf contrainte réglementaire, les documents qui ne sont pas nativement sous forme d'originaux électroniques et dont le format d'origine n'est pas reconnu comme pérenne au sens de la norme ISO14641, sont convertis, en PDF/A lorsque cette conversion est possible.

Dans le cas où cette conversion n'est pas possible le document reste dans son format d'origine.

Dans tous les cas, l'intégrité sera mise en œuvre par un scellement technique en s'appuyant sur le format le plus approprié :

- PAdES pour les formats PDF & PDF/A,
- XAdES pour les autres avec une signature enveloppante ou détachée.

Les documents nativement sur support papier seront traités comme précédemment indiqué.

#### **7.2.8.3.2.** b) Validation des documents soumis à un téléservice

Les documents pris en charge par le téléservice sont validés par une signature électronique ou une signature numérique, quel que soit leur format d'origine (papier ou électronique). Les documents principaux sous forme électronique font l'objet d'une signature électronique, lorsque cette dernière :

- est exigée par les lois et règlements,
- ou à défaut, lorsque le document papier substitué fait l'objet d'une signature manuscrite.

Les pièces justificatives nativement sous forme électronique, font l'objet d'une signature électronique, lorsque cette dernière :

- est exigée par les lois et règlements,
- ou à défaut, lorsque le document papier substitué fait l'objet d'une signature manuscrite.

Les pièces justificatives numérisées ne reçoivent pas de signature électronique (de type juridique).

Les formats de signature acceptés et utilisés par un téléservice sont les suivants :

- Basiques : CMS/PKCS7, XMLDSig, PDF, S/MIME
- Avancés : CAdES, XAdES, PAdES

#### **7.2.8.3.3.** c) Préparation et transmission électronique

Il y a lieu de :

- Vérifier la liaison entre document principal et pièce justificative,
- Contrôler des certificats électroniques avant émission

- Créer un "paquet d'envoi" constitué par la réunion de tous les fichiers traités dans une même session accompagnés de données de service, notamment de sécurisation (certificats, signatures),
- Ouvrir une session de transport
- Organiser le routage des flux et leur limitation.

#### **7.2.8.3.4.** d) Journalisation et archivage

##### a. Journalisation

Toutes les opérations effectuées par le téléservice sont journalisées automatiquement avec les éléments d'authentification des opérateurs et un horodatage local afin d'être en mesure de fournir une preuve à toutes requêtes. La fonction de journalisation du téléservice consiste à enregistrer tous les faits et actions ainsi que l'environnement d'exploitation. Le processus de journalisation est effectué en tâche de fond et doit permettre un enregistrement en temps réel des opérations effectuées. Il est incontournable au sens de l'exploitation et n'est pas modifiable.

L'écriture dans les journaux est automatique, elle est une conséquence des contrôles des droits d'accès. Les enregistrements ne sont pas modifiables a posteriori car la protection s'appuie sur le chaînage des journaux, un scellement technique journalier et l'archivage de chaque journal dans un coffre-fort électronique ou un SAE (Système d'archivage électronique).

##### b. Archivage électronique

Le téléservice met en œuvre un archivage électronique à vocation probatoire permettant l'archivage électronique de tout objet numérique. Cet archivage est de nature à garantir l'intégrité dans le temps des données à partir de 2 prestations complémentaires : une GED (Gestion Électronique des Documents) en charge de l'indexation et du classement, un SAE (Système d'archivage électronique) en charge du cycle de vie du document, plus particulièrement sa durée de conservation en accord avec la politique d'archivage. Les conditions et modalités de l'archivage électronique du téléservice sont spécifiées dans la Politique d'Archivage.

### **7.2.8.4. 3) Les moyens de sécurisation du téléservice**

#### **7.2.8.4.1.** a) Les moyens basiques

En ce qui concerne les moyens de sécurisation déployés par le téléservice, ils s'appliquent tant à la phase de dématérialisation et ses opérations connexes et éventuellement, qu'à la phase de

sécurisation des échanges électroniques. La source principale de ces exigences est le référentiel général de sécurité (RGS, OID, version/date).

Notamment sont considérées : l'identification et l'authentification. Pour la confidentialité, aucune mesure de chiffrement ne sont appliquées à ces objets sur le téléservice pour garantir leur confidentialité. Cependant les données personnelles susceptibles d'être présentes dans ces objets sont protégées par les dispositions de la loi n° 2017-20 sur la protection des données à caractère personnel.

#### **7.2.8.4.2.** b) Les moyens complémentaires

Horodatage : Les objets circulants sur le téléservice ne font l'objet d'aucun horodatage spécifique à l'exception des cas où la réglementation nécessite l'apposition d'une date certaine.

Disponibilité : la disponibilité d'un téléservice est garantie 24 heures sur 24 et 7 jours sur 7, sauf pour dans les cas ou les circonstances prévus les contrats de service et/ou le PRC / PCA.

Interopérabilité : les échanges électroniques transportés par le téléservice respectent le RGI (OID, numéro de version/date).

#### **7.2.8.4.3.** c) Sécurisation des terminaux et serveurs

La sécurité offerte sur les postes de travail répond aux objectifs généraux de sécurité suivants :

- Identification et authentification des utilisateurs des terminaux,
- Gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôle par rôle et nom d'utilisateur),
- Protection contre les virus informatiques,
- Journalisation des événements,
- Un dossier technique précisant particulièrement la description précise et les numéros de série des matériels et des logiciels mis en œuvre au sein d'un téléservice.
- Intégrité des logiciels liés à un téléservice.

Le téléservice inclut des mécanismes assurant la détection et la prévention des attaques du réseau provenant des réseaux auxquels il est raccordé, en particulier d'Internet. Ces mécanismes sont conformes à l'état de l'art en matière de prévention des intrusions. La documentation de mise en œuvre et d'exploitation du dispositif prévoit que ces mécanismes font l'objet de mises à jour régulières conformément aux prescriptions des éditeurs de ces mécanismes.

#### **7.2.8.4.4.** d) Sécurisation des flux par signature

### c. Signature numérique et signature électronique

Les signatures numériques sont employées à chaque fois qu'il est nécessaire de garantir la sécurisation des échanges électroniques. Elle satisfait aux exigences suivantes :

- Être propre au signataire ;
- Permettre d'identifier le signataire ;
- Être créé par des moyens que le signataire puisse garder sous son contrôle exclusif
- Garantir le lien avec les documents ou fichiers auxquelles elle s'attache, de telle sorte que toute modification ultérieure de ces factures soit détectable.

La signature électronique, qui garantit les effets juridiques, repose sur un certificat électronique qui est délivré par un prestataire de service de certification. Une signature électronique est appliquée à tout fichier ou document dont la version papier comporterait une signature manuscrite.

### d. Type de certificat électronique en support de la signature

Le certificat électronique pour la transmission des flux comporte au minimum les informations listées par la législation.

### 7.3. La gouvernance de l'urbanisation et la gestion des projets digitaux

La gestion de projet recouvre les processus et activités de planification, d'organisation, de gestion et de contrôle des ressources (humaines, financières et matérielles), des procédures et des protocoles en vue d'atteindre des objectifs spécifiques dans un délai imparti.

Un projet comporte un début et une fin et il est destiné à aboutir à un produit, un service ou un résultat. Il désigne par conséquent des mécanismes importants permettant d'apporter un changement au sein d'une institution ou d'un environnement.

La nature temporaire des projets s'oppose aux opérations habituelles qui sont des activités fonctionnelles répétitives, permanentes ou semi-permanentes permettant d'obtenir des produits ou des services. Dans les faits, les gestions de ces deux systèmes sont souvent sensiblement différentes l'une de l'autre et elles nécessitent donc le développement de compétences techniques et de stratégies de gestion distinctes.

Dans un contexte de digitalisation de service publics, la production réussie de « services publics digitalisés » implique généralement des réformes et des initiatives de modernisation des SI gouvernementaux, qui sont intégrés dans les activités courantes des interactions avec les différents usagers du SI de l'Etat notamment les citoyens, les entreprises, les associations. La première difficulté de la gestion de projet réside dans la nécessité de parvenir à un résultat qui corresponde aux buts et aux objectifs du projet et à une qualité définie, en respectant les contraintes de coûts/ressources disponibles, et de délai.

#### **LE PILOTAGE DU SI S'EXERCE PAR LE BIAIS D'INSTANCES DE GOUVERNANCE PRESIEES PAR UN DIRECTEUR METIER ET COMPETENTES SUR UN PERIMETRE ET UN NIVEAU D'ORGANISATION DEFINIS**

Les principes généraux de la gouvernance attribuent un rôle central aux métiers. On associe pour chaque rôle une responsabilité, les métiers sont les commanditaires et bénéficiaires des systèmes d'information. Le métier assure la maîtrise d'ouvrage du SI dont il est bénéficiaire et assure à ce titre :

- l'expression des nouveaux besoins métier et de leur justification ;
- la validation des solutions SI proposées ;
- le financement des solutions SI ;
- les recettes de conformité des solutions livrées.

Le métier est garant de la bonne articulation du SI au sein de ses processus métier et de son organisation en veillant à :

- l'évolution et adaptation des organisations et procédures ;
- l'accompagnement du changement associé à une nouvelle solution SI ;
- suivi de la performance des processus métier.

La **fonction SI** vient en support des métiers de l'organisation, elle est en charge :

- d'assurer le maintien en conditions opérationnelles (MCO) conformément aux niveaux de services convenus avec les métiers (continuité, sécurité, qualité ...) ;
- de proposer, concevoir et mettre en œuvre les évolutions du SI en fonction des besoins d'alignement du SI par rapport aux évolutions stratégiques des métiers, d'amélioration des processus, d'évolution des organisations, d'évolutions réglementaires et des évolutions technologiques ou de rationalisation d'architecture du SI.

Dans ce cadre la **fonction SI** est redevable des coûts, des délais, de la qualité, de l'évolutivité du SI sur le périmètre dont elle a la charge. Elle est garante de la pertinence et de la pérennité des choix technologiques. Le système d'information est le résultat d'un travail réalisé en partenariat entre les

métiers et la **fonction SI**, chaque « discipline » y apportant ses compétences et les responsabilités associées

Une recherche constante d'optimisation entre proximité métier et mutualisation, Les systèmes d'information doivent d'une part délivrer un service au plus près des besoins métiers et de leurs spécificités, mais également satisfaire aux exigences d'interactions entre les SI, de sécurité, de disponibilité, ainsi que de maîtrise des coûts. Ces exigences impliquent une recherche de cohérence d'ensemble, de standardisation de solutions lorsque celles-ci ne constituent pas un facteur différenciant pour le métier, ou encore de mutualisation de moyens.

Cette recherche d'optimisation entre proximité métier d'une part, et standardisation et mutualisation d'autre part, se traduit par :

- des politiques et un cadre d'urbanisation des systèmes d'information de l'Etat ;
- la mutualisation de moyens en centres de services partagés (CSP), ou centres d'expertises, pilotés par des entités transverses notamment pour la gestion des infrastructures SI ou le partage de compétences clés ;
- une logique de proximité métier pour les développements et la maintenance soit au niveau de chaque entité opérationnelle, soit au sein d'une entité mutualisée entre plusieurs entités.

### **7.3.1. Rappel du cadre d'urbanisation des systèmes d'information de l'Etat**

Le cadre d'urbanisation des systèmes d'information est l'outil pour le pilotage stratégique et opérationnel du patrimoine SI de l'Etat et doit à ce titre être élaboré dans une démarche inclusive et consensuelle en associant les représentants de tous les ministères et les établissements publics.

Le cadre d'urbanisation des SI sera élaboré en se basant sur les résultats des groupes de travail. Ces conclusions empiriques seront structurées en se référant au Framework TOGAF qui est considéré comme le cadre d'urbanisation et d'architecture le plus utilisé par les entreprises et les gouvernements. TOGAF « The Open Group Architecture Framework » étant une méthode générique comportant des solutions clés en main à la transformation de l'architecture d'entreprise et l'outil d'urbanisation par excellence. Il fournit une grille d'analyse de l'existant, d'élaboration du cadre d'urbanisation et de la conception des Architectures technique et fonctionnelle pour la mise en place d'un système de digitalisation des services publics et des paiements y afférents.

La DGTIC du MESRSTIC a élaboré un cadre d'urbanisation des systèmes d'information comprenant les sections suivantes :

- un cadre général d'urbanisation des systèmes d'information de l'Etat ;
- un cadre général d'interopérabilité des systèmes d'information de l'Etat;
- un cadre général du référentiel des données de l'Administration ;
- et un cadre général de la sécurité des systèmes d'information de l'Etat.

#### **CGRD – Cadre Général des Référentiels des Données**

L'enregistrement et le traitement de la donnée sont la manifestation d'une transaction (paiement, déclaration de revenus, ...), d'une réalité physique (information topographique par exemple), d'un objet légal (cadastre, immatriculation des entreprises, ...), d'une relation de service (demande d'information, inscription, ...), d'une décision (autorisation, gestion de droits et d'habilitation, ...).

L'automatisation de plus en plus systématique des processus donne un rôle prépondérant à la donnée numérique et dans un nombre croissant de cas, la donnée numérique est devenue la seule manifestation et la seule trace de la transaction, de la décision, de l'objet légal.

Les données constituent un des principaux actifs stratégiques de l'État.

Considérer la donnée comme un actif nous invite à considérer les questions suivantes : Comment optimiser son coût d'acquisition ? Comment entretenir cet actif et créer le maximum de valeur avec cet actif ? Comment le partager efficacement ?

Le recueil de données présente un coût d'acquisition pour l'État, quelle que soit la méthode (téléservices, saisie en guichet, capteurs sur le terrain, achat en masse d'informations à un tiers...), d'autant plus s'il est nécessaire de disposer d'informations de qualité (fiable, sans doublon, ...), ce qui peut nécessiter vérification, recoupement, retraitement, ... ; au-delà du coût pour l'État, ce recueil présente, le cas échéant, un coût pour celui qui la fournit (l'utilisateur, l'entreprise).

Il vient alors naturellement à l'esprit qu'il est nécessaire d'optimiser ce recueil :

- Eviter de recueillir plusieurs fois les mêmes données. A l'échelle de l'État, cela conduit immédiatement aux initiatives de type « dites-le nous une fois », et à chercher à mettre en commun les données entre plusieurs administrations, et à choisir des données utiles au plus grand nombre, dans des formats pertinents.
- Eviter autant que possible les saisies, les ressaisies, les intermédiations, ... et privilégier l'interconnexion avec les systèmes d'information existants au plus près de la source de référence. Pour le système d'information de l'État, cela signifie qu'il doit s'ouvrir à ses partenaires au travers notamment d'interfaces « de système à système » et développer une vision du système d'information au-delà de ses frontières de responsabilité.

Pour l'État, la valorisation de cet actif s'entend de nombreuses manières :

- La donnée doit être disponible et accessible à toutes les administrations qui en ont opérationnellement besoin, de façon documentée, avec des mécanismes de connexion simples à mettre en œuvre,
- La donnée doit être disponible pour être traitée à des fins décisionnelles, notamment pour l'évaluation des politiques publiques.
- Au-delà des administrations et de ses opérateurs, les données qui ne présentent pas de sensibilité particulière quant à leur confidentialité, ont vocation à être mises à disposition de tiers (Open Data).

Bien entendu, la valeur qui peut être créée dépend de nombreux facteurs, notamment de « qualité » : les données sont-elles complètes, exactes, cohérentes ? Peut-on y accéder facilement, peut-on les mettre à jour facilement ? Leur disponibilité, leur intégrité font-elles l'objet d'un engagement ?

Cette qualité dépend des processus de création, de mise à jour, de suppression des données ; elle dépend également des fonctionnalités d'accès mises en œuvre, de leur structure, de leur format. Elle dépend enfin de la confiance que le destinataire des données peut avoir globalement en y accédant, c'est-à-dire, au-delà des aspects techniques, elle dépend des engagements de service, de la gouvernance et de l'organisation en place.

Il est donc essentiel que l'État se dote de règles de Gouvernance des Données, intégrant des dimensions techniques, fonctionnelles, métiers et organisationnelles, et les applique progressivement dans l'ensemble de son système d'information.

Le Cadre Général des Référentiels de Données (CRGD), a pour ambition de fixer le corpus des règles, destinées en particulier à la gestion des Données de Référence et des dispositifs qui les gèrent, appelés « Référentiels de Données ».

Dans ce rapport on présente les objectifs du cadre, son périmètre d'emploi, son articulation avec le *Cadre Général d'Urbanisation du SI de l'État*, son processus interministériel d'élaboration et d'approbation. Ensuite on expose un certain nombre de définitions et de notions essentielles, en insistant en particulier :

- Sur la modélisation sémantique, travail conceptuel indispensable à une compréhension partagée entre les acteurs, en s'appuyant autant que possible sur les normalisations existantes et sur des outils de modélisation,
- Sur les différents critères de qualité de la donnée,
- Sur ce qui est attendu d'un Référentiel de Données,
- Sur l'articulation avec la démarche d'urbanisation

### **CGU – Cadre Général d'Urbanisation**

Dans toutes les activités de l'Etat, au niveau central, comme au niveau déconcentré, l'utilisation de moyens d'échange, de traitement, d'analyse et de restitution de données ou de documents de toutes natures, est devenu primordial. Ces moyens, leurs organisations et leurs entretiens conditionnent la plupart du temps la performance globale de l'administration, et donc des politiques publiques.

Ces systèmes d'information et de communication (SIC) sont omniprésents dans la sphère publique. Ils sont interconnectés et interdépendants entre eux au sein de l'Etat, mais aussi et surtout interconnectés avec l'ensemble de l'écosystème de l'Etat : les opérateurs ou tous types d'établissements partenaires de l'Etat, les collectivités territoriales, les instances spécifiques au niveau du pays, ou internationale, enfin et surtout avec les usagers eux-mêmes, qu'ils soient particuliers, professionnels, associations, ou entreprises. Ces moyens, enrichis des innovations de ces dix dernières années, deviennent ainsi particulièrement prégnants dans toutes les relations qu'elles soient internes ou externes à l'Etat.

La mise en place de la Direction Générale des Technologies de l'Information et de la Communication (DGTIC), renforcée par l'élaboration de la Stratégie Nationale de Modernisation de l'Administration et des TIC, définit une première gouvernance interministérielle et les orientations stratégiques concernant la transformation du système d'information (SI) de la République Islamique de la Mauritanie.

Au-delà du cadre stratégique, il est primordial également d'organiser et maîtriser cette transformation du SI, en recherchant continuellement à :

- le simplifier, en particulier vis à vis des utilisateurs internes (agents) et externes (collectivité, usagers, entreprises...);
- optimiser l'organisation des ressources elles-mêmes (techniques, financières, humaines);
- le rendre plus réactif et plus flexible par rapport aux évolutions de son environnement.

C'est l'objectif de la démarche d'urbanisation du SI de l'Etat, qui s'inspire de la pratique de l'urbanisation des villes. Cette démarche contribue directement à la transformation du SI de l'Etat. Elle doit permettre d'aligner le système d'information et de communication sur la stratégie de l'Etat, ses évolutions et ses champs de contraintes, dans un cadre formel, compréhensible et partagé. L'urbanisation du SI de l'Etat est l'outil pour le pilotage du patrimoine SI et une aide à la décision pour toutes les actions de transformation.

Cette démarche d'urbanisation n'est pas le travail de quelques experts, mais bien une démarche collective. L'urbaniste SI est l'acteur chargé de préparer, de coordonner, d'animer et de suivre cette démarche, sous la responsabilité des métiers et des DSI avec les autres acteurs SI (tels que les chefs de projets MOA/MOE, les architectes techniques, les expert méthode et qualité, etc.). C'est la raison fondamentale qui a poussé à l'élaboration de ce Cadre Général d'Urbanisation du SI de l'Etat. C'est le deuxième changement de paradigme. Il décrit avant toute chose le cadre de coopération de l'ensemble des différents contributeurs à la démarche : métiers, projets et DSI. Plutôt que de décrire un cadre sous la forme de méthodes, de règles, et d'outils nécessaires, il pose les principes fondateurs de la démarche qui doivent inspirer toutes les actions de transformation du SI de l'Etat. Ces principes portent sur l'ensemble des facteurs impactant la transformation du SI de l'Etat à savoir : la coopération entre les acteurs, la gouvernance du SI, la gouvernance des données, la conception des composants du SI, des interfaces et des échanges, la conception des services pour les utilisateurs (agents ou usagers), la gestion des applications, des infrastructures et enfin, véritable épine dorsale de la démarche, sur la gestion de la connaissance sur le patrimoine SI.

Au-delà des principes et donc du « pourquoi » d'une telle démarche, le cadre définit les grandes activités de la démarche et les principaux livrables, sans rentrer dans des choix organisationnels propres aux ministères et administrations.

La trajectoire du SI de l'Etat sera l'un des principaux livrables de cette démarche. Elle décrit la dynamique d'évolution du SI de l'Etat. Elle sera le support pour les décisions ou arbitrages sur la transformation du SI de l'Etat. Elle décrit comment le portefeuille d'initiatives et de projets de chaque ministère impactent le SI de l'Etat, et contribuent à atteindre une cible rationalisée et définie. Ce travail de co-construction de la trajectoire du SI de l'Etat, avec l'ensemble des ministères, s'inscrit durablement dans le temps, dans une dynamique d'amélioration continue.

Cette trajectoire s'appuie sur une des nomenclatures clés de la démarche : le Plan d'Occupation des Sols du SI de l'Etat, cartographie fonctionnelle de l'ensemble du SI de l'Etat.

Il s'agit de fédérer les pratiques actuelles en matière de transformation, et d'architecture du SI de l'Etat, de les enrichir mutuellement en leur donnant un cadre de travail formel. Il n'est pas question de contraindre, mais bien de mettre en commun, et de rechercher les méthodes de travail adaptées aux besoins des différents ministères et administrations, en utilisant toutes les meilleures pratiques du moment qu'elles soient internes à l'Etat, ou issues de pratiques reconnues mondialement. L'objectif de cette démarche est de construire les conditions favorables de coopération entre les acteurs concernés dans la transformation du SI de l'Etat. L'objectif est également de tirer les pratiques vers le haut en définissant un niveau de maturité minimal qui garantisse la pérennité de la démarche elle-même et l'atteinte des objectifs de maîtrise de la transformation du SI de l'Etat.

### **CGS – Cadre Général de Sécurité**

En guise du chantier de Digitalisation des services, ce cadre général de sécurité élaboré est destiné aux différentes administrations et entités de la République Islamique de Mauritanie.

Il constitue la référence des directives et exigences en termes de sécurité des Systèmes d'informations de la République Islamique de Mauritanie.

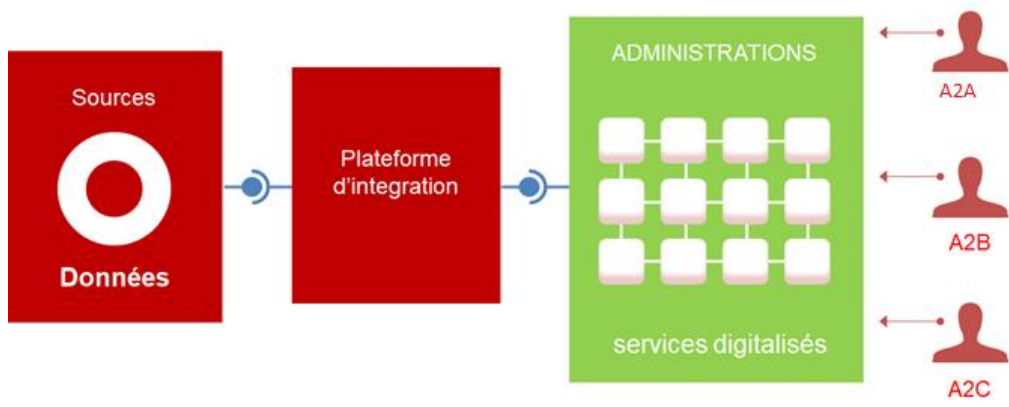
Il détermine les mesures et exigences de sécurité d'information qui doivent être implémentés et suivis par les différentes administrations de la République Islamique de Mauritanie.

### **CGI – Cadre Général d'Interopérabilité**

Le CGI traite des questions d'interopérabilité dans les différents cas illustrés dans le schéma ci-après. Le terme « Autorité Administrative » ou « AA » définit une organisation publique au sens large. Cela peut être une Administration générale, un service territorial déconcentré, un établissement public sous tutelle, une collectivité territoriale, un organisme de la protection sociale, ou de la sphère hospitalière :

Trois principaux cas sont identifiés :

- Les échanges entre autorités administratives : A2A.
- Les échanges entre une autorité administrative et une entreprise (au sens large, une unité légale, que ce soit une entreprise, une personne physique, une association) : A2B
- Les échanges entre une autorité administrative et un citoyen : A2C



### **7.3.2. La gouvernance du cadre d'urbanisation des systèmes de l'information de l'Etat**

*La gouvernance de l'urbanisation et de l'architecture des systèmes d'information se matérialise très souvent par la mise en place d'un bureau de Design Authority (l'autorité de conception). Ce comité transverse à porter par la DGTIC du MESRSTIC aura pour mission de mettre en œuvre et d'animer les recommandations, les règles et les normes définies dans les documents du cadre d'urbanisation des systèmes d'information de l'Etat.*

#### **La mission et les rôles du Comité d'Architecture :**

Le rôle du comité d'architecture est transverse à l'ensemble des entités publiques, il supervise la mise en œuvre de la stratégie de gouvernance de l'architecture, les objectifs fondamentaux et les responsabilités du comité d'architecture sont :

- fournir les bases à tous les processus de décision en rapport avec les architectures
- garantir la cohérence entre les sous-architectures
- définir des cibles de réutilisation de composants techniques
- définir le degré de flexibilité de l'architecture pour s'adapter aux besoins changeants et aux potentiels des nouvelles technologies
- faire respecter la conformité d'architecture et les règles de sécurité et d'interopérabilité
- améliorer le niveau de maturité de la discipline d'architecture et de sécurité
- s'assurer que les réalisateurs adoptent bien une démarche guidée par l'architecture et par la sécurité
- expliciter les règles d'escalade pour les décisions exceptionnelles

Toutefois une partie opérationnelle est nécessaire pour le comité :

- suivi du contrat d'architecture
- réunions régulières
- implémentation et gestion efficace et cohérente des architectures
- résolution des ambiguïtés et conflits
- conseil, orientations, information
- conformité aux architectures, dérogations pertinentes avec la stratégie
- changements de politiques si des dérogations s'accumulent
- publication des informations des contrats sous contrôle
- vérification des niveaux de service réels, des économies de coûts effectives, etc.

Pour mettre en place ce comité, nous recommandons de mettre en place une de 3 à 5 architectes. Ce comité doit être organisé pour son fonctionnement, comme mettre en place des méthodes de travail, bonnes pratiques, des objectifs de gouvernance, un planning etc...

#### **Conformité d'Architecture :**

Il est primordial de vérifier la conformité de chaque architecture et pour chaque projet SI, pour cela il faut développer les vues qui mettent en évidence les impacts du projet sur l'architecture des SI de l'Etat et effectuer des revues de conformité d'architecture pour chaque projet, ces revues qui ont pour but :

- Repérer les erreurs d'architecture le plus tôt possible afin de réduire les coûts et les risques d'un changement plus tard dans le cycle de vie du projet
- S'assurer de la mise en œuvre des bonnes pratiques de développement de l'architecture
- Fournir une vue générale de la conformité aux normes et aux standards décrits dans le cadre d'urbanisation des SI de l'Etat.
- Identifier si les standards eux-mêmes demandent une évolution
- Identifier les services d'une application qui pourraient faire partie de l'infrastructure de l'entreprise

- Lister les stratégies de coopération, de partage de ressources et d'autres synergies entre les diverses équipes d'architecture
- Utiliser les potentiels des nouvelles technologies
- Identifier les critères-clefs d'achat de composants, dont les logiciels
- Identifier les écarts d'architecture significatifs et les communiquer aux éditeurs de produits et de services

Pour la revue de conformité un certain nombre de vérifications doit être effectué via des checklists, comme par exemple : checklist matériels et des logiciel de base, checklist des applications, des services logiciels et middleware, checklist de la sécurité, checklist de l'administration système, checklist des méthodes et outils de l'ingénierie.

### 7.3.3. Quelques principes de gestion des projets SI

La gestion de projet recouvre les processus et activités de planification, d'organisation, de gestion et de contrôle des ressources (humaines, financières et matérielles), des procédures et des protocoles en vue d'atteindre des objectifs spécifiques dans un délai imparti.

Un projet comporte un début et une fin et il est destiné à aboutir à un produit, un service ou un résultat. Il désigne par conséquent des mécanismes importants permettant d'apporter un changement au sein d'une institution ou d'un environnement.

La nature temporaire des projets s'oppose aux opérations habituelles qui sont des activités fonctionnelles répétitives, permanentes ou semi-permanentes permettant d'obtenir des produits ou des services. Dans les faits, les gestions de ces deux systèmes sont souvent sensiblement différentes l'une de l'autre et elles nécessitent donc le développement de compétences techniques et de stratégies de gestion distinctes.

Dans un contexte de digitalisation de service publics, la production réussie de « services publics digitalisés » implique généralement des réformes et des initiatives de modernisation des SI gouvernementaux, qui sont intégrées dans les activités courantes des interactions avec les différents usagers du SI de l'Etat notamment les citoyens, les entreprises, les associations. La première difficulté de la gestion de projet réside dans la nécessité de parvenir à un résultat qui corresponde aux buts et aux objectifs du projet et à une qualité définie, en respectant les contraintes de coûts/ressources disponibles, et de délai.

Ci-dessous on va détailler les principales thématiques cadrant la gestion de projet de bout en bout en se basant sur l'une des principales références de gestion de projets reconnue mondialement et adaptée également au contexte de projets dans le cadre d'un SI gouvernemental qui est le PPMI-PMBOK (Project Management Institute – Project Management Body of Knowledge)

Thématiques	Règles de l'art	Exemples de bonnes pratiques
Pilotage Global (Intégration)	<p><b>Clarifier les objectifs du projet, documenter ses principaux paramètres fonctionnels, techniques et organisationnels :</b></p> <ul style="list-style-type: none"> <li>Partager une vision commune avec tous les acteurs</li> <li>Elaborer une charte et un plan de projet selon l'ampleur, la complexité et la vulnérabilité du projet pour documenter le projet et communiquer</li> </ul>	<ul style="list-style-type: none"> <li>"Mettre en œuvre les pratiques Agile : Les individus et leurs interactions plus que les processus et les outils Des logiciels opérationnels plus qu'une documentation exhaustive La collaboration avec les clients plus que la négociation contractuelle L'adaptation au changement plus que le suivi d'un plan"</li> <li>Utiliser le management visuel accessible à tous</li> <li>Piloter par la valeur</li> <li>Organiser une réunion de lancement significative avec l'ensemble des intervenants, si possible en physique</li> <li>Formaliser un plan de projet (structures de pilotage, modèle de production...), le plus concis possible et utile à la communication</li> <li>Mettre en œuvre un reporting performant en concertation avec les acteurs et avec les outils associés</li> </ul>

Contenu	<p><b>Assurer la maîtrise de ce qui est inclus et non inclus dans le contenu du projet :</b></p> <ul style="list-style-type: none"> <li>• Réaliser le projet dans les limites prescrites (budget, délai, contenu, qualité)</li> <li>• Assurer que les exigences sont respectées et répondent aux besoins de tous les acteurs</li> <li>• Assurer rapidement l'optimisation et la disponibilité des ressources</li> <li>• améliorer la satisfaction des clients et le moral des équipes du projet</li> </ul>	<ul style="list-style-type: none"> <li>• Intégrer les utilisateurs dès le démarrage du projet, planifier des phases de démonstration pour valider les hypothèses, la construction en cours et les ajustements à prendre en compte</li> <li>• Utiliser une matrice des compromis et la partager avec tous les acteurs</li> <li>• Nommer 1 Product Owner (représentant du client) unique, légitime et disponible (à plein temps)</li> <li>• Intégrer le changement, adapter le produit ou le service et le plan projet en conséquence.</li> <li>• Démarrer le projet sur une ébauche (Minimum Viable Product) pour valider les hypothèses principales avec le client.</li> <li>• Intégrer les impacts non fonctionnels (dette technique, exploitabilité, sécurité, DEVOPS...) dès le démarrage, avec les experts concernés.</li> <li>• Inclure dans le contenu (backlog, périmètre) les items fonctionnels et non fonctionnels (dette technique, exploitabilité, sécurité, DEVOPS...) et le partager avec les acteurs</li> <li>• Intégrer la migration et la qualité des données dans le projet comme une étape à part entière</li> <li>• Faire valider l'architecture technique et fonctionnelle dans les instances appropriées</li> <li>• Mesurer le gain « produit/service » obtenu à chaque livraison</li> </ul>
Délai	<p><b>Gérer l'exécution et l'achèvement du projet dans le temps voulu</b></p> <ul style="list-style-type: none"> <li>• Planifier le projet en collaboration avec l'équipe et les parties prenantes</li> <li>• Suivre l'avancement du projet et ajuster la planification</li> <li>• Mesurer la performance, mettre en œuvre des mesures de corrections ou d'ajustement</li> </ul>	<ul style="list-style-type: none"> <li>• Donner accès facilement à l'avancement du projet pour tous les intervenants</li> </ul>
Coûts	<p><b>Estimer et surveiller les coûts</b></p> <ul style="list-style-type: none"> <li>• Conserver le coût total du projet sous la limite du budget validé</li> <li>• L'équipe participe à l'estimation du projet</li> </ul>	<ul style="list-style-type: none"> <li>• Réaliser la planification et les estimations avec l'équipe projet</li> </ul>
Ressources humaines	<p><b>Organiser, développer et soutenir l'équipe projet</b></p>	<ul style="list-style-type: none"> <li>• Rédiger une charte d'engagement avec les règles de vie de l'équipe</li> </ul>

	<ul style="list-style-type: none"> <li>• Identifier les rôles, les responsabilités, les compétences requises et le mode de fonctionnement de l'équipe avec tous ses membres</li> <li>• Confirmer les disponibilités et obtenir les ressources nécessaires</li> <li>• Améliorer les compétences de l'équipe, ses interactions et son environnement global</li> <li>• Suivre la performance de l'équipe, lui fournir les informations nécessaires, l'aider à résoudre les problèmes et gérer les modifications nécessaires pour optimiser la performance du projet</li> </ul>	<ul style="list-style-type: none"> <li>• Définir avec les acteurs une raison d'être du projet pour fédérer l'équipe autour d'objectifs communs</li> <li>• Organiser des rencontres en physique avec les intervenants</li> <li>• Donner l'autonomie nécessaire à l'équipe sur son périmètre. L'équipe doit réfléchir à intervalles réguliers (rétrospectives) aux moyens de devenir plus efficace et adapter son mode de fonctionnement en conséquence.</li> <li>• Clarifier les rôles et les responsabilités, si possible mettre en place des binômes pour permettre des back up quand nécessaire</li> <li>• S'assurer de la bonne santé de l'équipe au fil du projet, vérifier que des temps de récupération et de convivialité sont prévus</li> <li>• Les softskills font parties du cursus de formation pour le manager et l'équipe : assertivité, droit à l'erreur, feedback, bienveillance, pratiques de management agile ...</li> </ul>
Communication	<p><b>produire, réunir, diffuser, archiver et éliminer définitivement l'information sur le projet, adéquatement et au moment opportun.</b></p> <ul style="list-style-type: none"> <li>• Définir les besoins en information des intervenants au projet et établir un moyen adéquat d'y répondre</li> <li>• Rendre l'information disponible à tous les intervenants au projet, au bon moment</li> </ul>	<ul style="list-style-type: none"> <li>• L'information sur le projet est disponible dans un référentiel unique accessible à tous les intervenants</li> <li>• Planifier, organiser les communications sur le projet en accord avec les acteurs</li> </ul>

Risques	<p><b>Veiller à ce que les risques liés au à la solution soient identifiés, évalués et gérés de manière systématique au fil du projet</b></p> <ul style="list-style-type: none"> <li>• Évaluer et surveiller les risques</li> <li>• répondre aux risques</li> <li>• communiquer avec les intervenants et les consulter au sujet des risques</li> </ul>	<ul style="list-style-type: none"> <li>• Tester rapidement une hypothèse, quitte à se planter et pivoter, plutôt que d'évaluer longuement l'alternative.</li> <li>• Le droit à l'erreur est une valeur partagée avec l'équipe pour favoriser l'expérimentation, l'innovation et la confiance. Ce qui permet de tester ce qui est risqué au plus tôt et lever les risques au fil de l'eau</li> <li>• Intégrer les risques sécurité dès le démarrage du projet</li> <li>• Les opportunités et les éléments facilitateurs sont identifiés et renforcés</li> <li>• l'ensemble des intervenants contribue à l'identification des risques éventuels</li> <li>• Les risques organisationnels sont traités avec l'ensemble de l'équipe</li> </ul>
Approvisionnement	<p><b>Gérer les achats ou acquisitions des produits, des services ou des résultats nécessaires et externes à l'équipe de projet.</b></p>	<ul style="list-style-type: none"> <li>• Le cahier des charges définissant les prestations externes est partagé pour construire le processus de livraison</li> <li>• Solliciter les experts pour aider à rédiger le cahier des charges</li> </ul>

	<ul style="list-style-type: none"> <li>documenter les décisions d'approvisionnement du projet, spécifier les approches et identifier les vendeurs potentiels.</li> <li>obtenir les réponses de vendeurs, sélectionner un vendeur et attribuer un contrat.</li> <li>gérer les relations fournisseurs, suivre les performances des contrats et, le cas échéant, apporter aux contrats les modifications et les corrections appropriées.</li> <li>finaliser chacun des approvisionnements du projet (close le contrat).</li> </ul>	
Parties prenantes	<p><b>Identifier et gérer la satisfaction des parties prenantes comme un objectif du projet.</b></p> <p><b>Gérer les effets du changement sur les utilisateurs</b></p> <ul style="list-style-type: none"> <li>identifier les personnes / groupes susceptibles d'affecter le projet, ou d'être affectés par celui-ci. Quels sont leurs intérêts, leur participation, leurs interdépendances, leur influence et leur impact potentiel sur la réussite du projet ?</li> <li>communiquer et travailler avec les parties prenantes pour satisfaire leurs besoins et leurs attentes, traiter les problèmes au fur et à mesure qu'ils se présentent et promouvoir une implication appropriée des parties prenantes tout au long du projet.</li> <li>créer et mettre en œuvre des plans de gestion du changement qui maximisent l'adoption et l'utilisation de la part des utilisateurs et les préparent à leur nouvel environnement de travail</li> </ul>	<ul style="list-style-type: none"> <li>Identifier les promoteurs et les détracteurs sur le projet</li> <li>Intégrer rapidement les utilisateurs et clients pour obtenir un feedback dès le début du projet</li> <li>Construire les différents éléments de stratégies du projet (qualification, phase pilotes, déploiement, intégration) avec les acteurs projet</li> <li>Identifier les impacts sur les processus métier</li> <li>Accompagner les utilisateurs sur la prise en main du produit</li> </ul>
Qualité	<p><b>Identifier les exigences à respecter pour la gestion du projet et la gestion du produit.</b></p> <ul style="list-style-type: none"> <li>identifier les exigences de qualité et les normes à respecter pour le projet et ses livrables, documenter comment le projet démontrera sa conformité aux exigences et aux normes de qualité appropriées</li> </ul>	<ul style="list-style-type: none"> <li>Identifier, produire et stocker les preuves nécessaires au contrôle qualité</li> <li>Solliciter le Risk Manager pour réaliser une analyse de risque sécurité</li> </ul>

### 7.3.4. Renforcement des capacités

Plusieurs formations sont nécessaires pour accompagner la mise en œuvre des cadres d'urbanisation et de sécurité des systèmes d'information de l'Etat.

Nous proposons les formations suivantes pour monter en compétence dans l'urbanisation et l'architecture de SI :

- Formation Architecture de systèmes d'information
- Formation Urbanisation de systèmes d'information
- Formation Architectures des NTIC
- Formation Architecture logicielle : Fondamentaux
- Formation Evolution de la DSI
- Formation Urbanisation et architecture des systèmes d'information
- Formation COBIT : Introduction
- Formation TOGAF®
- Formation ISO 27001
- Formation COBIT5 : Foundation
- Formation COBIT5 : Foundation + Implementation
- Formation COBIT5 : Implementation

#### 7.3.4.1. Formation en management des risques ISO31000

Cette formation a pour objectif de vous dispenser les connaissances nécessaires à la compréhension de la gestion du risque, selon la norme ISO 31000. Vous apprendrez l'ensemble des principes fondamentaux, des règles et des processus du management du risque. Cette formation vous dotera également des compétences et des meilleures pratiques pour conduire une gestion professionnelle du risque au sein d'une organisation ou d'une entreprise. Elle vous préparera à l'examen de certification PECB ISO 31000 Risk Manager, pour certifier votre aptitude à manager les processus liés aux risques dans une organisation.

Au terme de cette formation, vous saurez:

- Comprendre les concepts et processus fondamentaux du management du risque.
- Mettre en contexte la norme ISO 31000, la norme ISO/CEI 31010 et les autres règlements.
- Maîtriser les méthodes, techniques et pratiques pour gérer le risque au sein d'un organisme.
- Faire appliquer les lignes directrices de la norme ISO 31000.
- Cette formation est adaptée à tout type et toute taille d'organisation ou d'entreprise soucieuse de gérer les risques de façon optimale.

#### A qui s'adresse la formation ISO31000 management des risques ?

Cette formation est destinée aux gestionnaires, superviseurs, aux consultants en charge du management du risque dans un organisme. Et toute personne souhaitant acquérir des connaissances approfondies sur les principes fondamentaux, le cadre et les processus de management du risque conforme à la norme ISO 31000

#### Formation Cobit5

Cette a pour objectif de vous dispenser les connaissances nécessaires à l'implémentation de Cobit 5. La **formation COBIT2019** s'organise autour de cours théoriques et d'ateliers pratiques. Vous apprendrez les différents processus pour assurer une implémentation réussie, vous serez formé à la compréhension du langage utilisé par le référentiel et à l'appliquer dans une **gouvernance des systèmes d'information**. Cette formation vous préparera également aux connaissances et compétences

nécessaires à l'examen de certification délivrée par l'ISACA : « **COBIT 2019 – Implementation** » pour valider votre expertise.

A l'issue de cette formation, vous saurez :

- Comprendre les enjeux de l'implémentation.
- Comprendre l'apport du référentiel COBIT.
- Implémenter COBIT et mettre en place une gouvernance fédérée des systèmes d'information.
- Comprendre et utiliser les bonnes pratiques de l'audit informatique.

#### **A qui s'adresse la formation Cobit® 5**

Cette formation s'adresse aux professionnels et administrateurs IT qui souhaitent apprendre à implémenter COBIT 5, elle s'adresse également aux responsables de projets, responsables réseaux et informatiques, et auditeurs qui désirent maîtriser ou conseiller l'implémentation de COBIT 5.

Cette formation s'adresse aux profils suivants :

- Chef de Projet
- Directeur de Projets
- Directeur des Systèmes d'Information (DSI)

#### **7.3.4.2. Formation CRISC**

Dans un contexte de transformations profondes des organisations, de développement des environnements numériques, d'accélération des mutations technologiques et des grands projets que mènent nombre de sociétés et acteurs économiques, cette certification vous apportera de solides connaissances reconnues à l'international sur les enjeux actuels de maîtrise globale des risques en lien avec les systèmes d'information.

Cette certification, axée autour de la gestion des risques et de la maîtrise des systèmes d'information, s'appuie principalement sur deux composants : d'une part sur les enjeux d'ERM (Entreprise Risk Management) de gestion globale des risques et d'autre part sur les principes de gouvernance et de contrôle des systèmes d'information.

Elle permet d'approfondir ses connaissances, bonnes pratiques ou réflexes à avoir pour identifier, revoir, contrôler et piloter les risques liés aux évolutions de systèmes d'information.

Cette certification est la seule qui soit à croisée des enjeux d'ERM et des risques liés aux systèmes d'information, et facilitera votre positionnement d'acteur incontournable sur ces sujets dans votre entreprise ou votre organisation.

#### **A qui s'adresse la formation CRISC ?**

Professionnels des Systèmes d'Information, professionnels de la gestion des risques, analystes métier spécialisés en risques, directeurs de projets, responsables de la conformité, professionnels métier qui souhaitent maîtriser la gestion des risques IT ainsi que l'implémentation des contrôles au sein des systèmes d'information. la formation sera aussi utile pour les professionnels désirant obtenir la certification CRISC (Certified in Risk and Information Systems Control).

#### **7.3.4.3. Formation (BPMN) Business Process Model and Notation**

Le BPM (Business Process Management) se compose d'un ensemble de méthodes, d'outils et de technologies destinés à concevoir, mettre en œuvre et contrôler les processus opérationnels de l'entreprise.

BPMN (Business Process Modeling and Notation) offre l'opportunité de représenter les processus internes de l'entreprise. Les analystes créeront les copies de ces processus, les développeurs techniques mettront ces processus en forme et les managers gèreront et surveilleront ces processus.

L'automatisation des diagrammes et autres représentations graphiques par le BPMN facilitera la prise de décision et la compréhension des processus d'information entre ceux qui travaillent dans l'entreprise, ceux qui mettent en œuvre ces processus, les clients et les fournisseurs.

Les objectifs de cette formation sont de permettre aux candidats de:

- Découvrir la valeur ajoutée de la notation BPMN 2.0 dans la qualité de la modélisation
- Prendre conscience du BPMN comme un outil de communication et de contrôle interne
- Comprendre l'amélioration continue des performances de l'entreprise
- Améliorer les relations d'affaires entre les entreprises

#### **A qui s'adresse la formation BPMN**

- Les DSI et les informaticiens de la DSI
- Les managers et techniciens des différents services de l'entreprise

Cette formation s'adresse aux profils suivants :

- Architecte SI
- Directeur des Systèmes d'Information (DSI)
- Urbaniste SI

#### **7.3.4.4. Formation PMP**

La gestion de projet prend une part prépondérante dans les pratiques de gestion des entreprises. Malgré l'apparente facilité de la théorie, les chefs de projet praticiens se rendent compte de la difficulté de l'art. Un chef de projet n'atteint l'efficacité en toutes circonstances qu'avec quelques années d'exercice.

Pour valider la pertinence de l'expérience acquise, les associations de management de projet ont défini des dispositifs de certification de personnes.

Ces dispositifs ne sont accessibles qu'aux professionnels pouvant justifier d'une expérience minimale de durée.

Le PMI ® (Project Management Institute) a défini une certification appelée PMP ® (Project Management Professional) qui remporte un succès réel.

#### **7.3.4.5. Formation PRINCE2 Foundation et Practitioner :**

PRINCE2 (Projects IN Controlled Environments) est une méthode de gestion et de certification de projet qui se focalise sur trois points : l'organisation, la gestion et le contrôle du projet. Propriété d'AXELOS Limited, cette méthode est de plus en plus utilisée car elle favorise l'utilisation contrôlée des ressources et permet de gérer plus efficacement les projets et les risques. Le recours à PRINCE2 favorise en outre l'adoption d'un langage commun à tous les participants d'un projet. Les participants à cette formation se prépareront activement au passage des certifications PRINCE2 Foundation et Practitioner (passées durant la formation).

#### **A qui s'adresse la formation ?**

Ce niveau de qualification est particulièrement utile pour les Managers de Projet et pour les ressources impliquées dans la conception, le développement et la réalisation de projet: les membres du comité de projet, ceux des équipes de projet, les ressources chargées de l'assurance de projet, les membres du bureau de projet et le personnel de l'organisation impliqué dans des projets gérés par PRINCE2.

#### **7.3.4.6. Formation ISO 27001 Foundation**

La formation et la certification PECB ISO27001 démontrera que votre organisation a défini et mis en place les meilleures pratiques dans les processus de la sécurité de l'information.

Ces schémas s'appliquent aux organisations de toutes tailles dans le domaine de la technologie qui souhaitent sécuriser leurs systèmes de management.

#### **Les bénéfiques sont :**

- Une sensibilisation en matière de sécurité de l'information améliorée
- Une réduction des failles de sécurité
- Un avantage concurrentiel
- Démontre une crédibilité et une confiance
- Se conforme aux lois et aux règlements associés

#### **7.3.4.7. Certified Ethical Hacking CEH V10**

Cette formation de piratage éthique vous place au cœur d'un environnement pratique avec un processus systématique. Ici, vous serez exposé à une manière totalement différente d'aborder la sécurité de l'information dans une organisation : en la piratant ! Vous allez scanner, tester, pirater et sécuriser vos propres systèmes. Vous apprendrez les cinq phases du piratage éthique et les différentes manières d'approcher votre cible et de réussir à vous immiscer à chaque fois ! Les cinq phases comprennent la reconnaissance, l'obtention d'un accès, le recensement, le maintien de l'accès et la couverture de vos traces.

Les objectifs de cette formation sont :

- Connaître les options, les outils et les astuces d'un hacker
- Pouvoir se protéger de façon ciblée contre des attaques
- Pouvoir mettre immédiatement en pratique les connaissances acquises concernant l'identification et la résolution des failles de sécurité grâce aux nombreux exercices et scénarios

#### **A qui s'adresse la formation ?**

- Responsables sécurité
- Auditeurs
- Professionnels de la sécurité
- Administrateurs de site
- Toute personne concernée par la stabilité des systèmes d'information

#### **7.3.4.8. Formation ITIL® Foundation (Information Technology Infrastructure Library)**

ITIL est un ensemble de bonnes pratiques qui permettent d'optimiser la gestion des Services Informatiques. Largement approuvé et utilisé par les acteurs du marché, clients et fournisseurs, ce référentiel se présente sous la forme d'une collection de livres couvrant les différents aspects de l'activité de gestion des services informatiques. Cette formation a pour objectif d'appréhender ITIL® et d'en comprendre ses principaux aspects.

### **A qui s'adresse la formation ITIL Foundation ?**

Tout professionnel impliqué dans la gestion des services informatiques : les décideurs informatiques, les managers informatiques et métiers, les responsables réseau, les analystes et propriétaires de processus, les analystes métiers, les consultants, les intégrateurs, les responsables d'assistance et de support, les fournisseurs de services, les développeurs, les commerciaux.

### **7.3.4.9. Formation ITIL Practitioner**

L'approche didactique de la formation ITIL Practitioner conduit l'apprenant à pouvoir :

- Utiliser les concepts clés de l'ITSM qui constituent les moteurs de l'amélioration continue des services
- Appliquer les principes directeurs de l'ITSM dans un contexte réel
- Mettre en œuvre une approche d'amélioration continue (CSI) au sein d'une organisation
- Faire usage des mesures et indicateurs pour permettre et faciliter la démarche d'amélioration continue
- Communiquer efficacement pour permettre et encourager l'amélioration continue
- Contribuer à la gestion des changements organisationnels dans le cadre de l'amélioration continue

Cette formation permet aux candidats de passer l'examen de certification professionnelle ITIL Practitioner et d'être reconnu internationalement en tant que praticien ITIL™.

### **A qui s'adresse la formation ITIL Practitioner ?**

Cette formation s'adresse à toute personne impliquée dans, ou concernée par, la gestion des services informatiques et ayant déjà une connaissance certifiée de ITIL®. Professionnels voulant obtenir le statut professionnel de Praticien ITIL®.

Cette formation s'adresse aux profils suivants :

- Chef de Projet
- Directeur de Projets
- Directeur des Systèmes d'Information (DSI)
- Responsable informatique

### **7.3.4.10. Formation Urbanisation en Systèmes d'Information par Dawan**

**Le contexte et la problématique :**

- Les 4 principes utilisés : structuration, modélisation, factorisation, transformation
- Les principes de base d'un SI
- La structuration d'un SI (le modèle)
- L'importance de l'organisation
- Les approches top-down et bottom-up
- Les 3 grandes étapes pour réaliser un SI performant
- Comment cartographier le SI existant
- Comment bâtir le SI cible
- L'approche par composants
- Exemples d'intégration du SI existant dans le SI cible

- Le plan de convergence du SI existant vers le SI cible
- Les acteurs du SI et leurs missions
- Les principales définitions dans un SI : cohérence, cohésion, flexibilité, agilité, séabilité, stabilité, performance, scalabilité
- Les démarches de management : COBIT, ITIL, CMMI, les méthodes agiles, UnifiedProcess, TOGAF ; MDA
- Qu'est ce que l'urbanisation du SI ?
- Le positionnement de ces démarches
- Les besoins des entreprises ou des organismes
- La modélisation des besoins stratégiques
- Le schéma directeur pour la stratégie du SI
- Comment déterminer les besoins d'une société : le SI décisionnel
- Le Big Data
- L'expression des besoins et le suivi des exigences
- Travaux pratiques

### **Les architectures des systèmes et conclusion**

- Pourquoi architecturer les systèmes ?
- Comment bâtir les architectures des systèmes, l'architecture fonctionnelle, l'architecture technique
- L'architecture logicielle, l'implémentation, les architectures des applications des mobiles : les O.S., les types d'application et de communication, la persistance, la publication, les frameworks, la sécurité, le développement
- Exemple d'urbanisme pour les applications des terminaux mobiles
- Travaux pratiques