p. 11-30 5411

AFDS

Agence du Fonds de Développement Social

SYSTEME D' INFORMATION DE SUIVI DE LA LUTTE CONTRE LA PAUVRETE

*Contrat n° AFDS 01C/38/02
Crédit n° 3446 - SE*

2ème Rapport d'orientations techniques

El Hadji Mar GUEYE

Août 2003

LISTE DES ABBREVIATION ET SIGLES

ARFS :	Antenne Régionale du Fonds de Développement Social
LAN :	Local Area Network
SGBD-R :	Système de gestion de base de données relationnel
SQL :	Structured Query Language
DSRP :	Document de stratégie de la réduction de la pauvreté
MDS :	Ministère du Développement Social
MEF :	Ministère de l'Economie et des Finances
RPV :	Réseau privé virtuel
VPN :	Virtual Private Network
LS :	Liaison Spécialisée
IP :	Internet Protocol
RNIS :	Réseau Numérique à Intégration de Services
FDS :	Fond de Développement Social

Le présent rapport de propositions faisant suite à la première partie de l'étude doit, conformément aux termes de références, présenter des propositions de prise en charge des besoins identifiés et les choix techniques conséquents. A ce titre, il sera articulé autour de deux grandes parties :

- une première relative aux protocoles d'échanges
- une deuxième se rapportant à l'architecture technique du futur système

Nota : Les nouvelles orientations issues de la revue à mi parcours du projet de Fond de Développement Social

Au moment de la finalisation de ce deuxième rapport d'orientation technique, nous avons été conviés, dans le cadre de la revue à mi-parcours du projet Fond de Développement Social, à une réunion de présentation de l'étude à l'intention des experts de la Banque Mondiale.

Cette réunion s'est ainsi tenue dans les locaux de l'AFDS le Mardi 24 juin 2003, à laquelle j'ai pris part pour faire l'état des lieux du projet et exposer les scénarios d'architectures techniques auxquelles nous sommes parvenus à cette phase de l'étude.

Des différentes interventions qui ont suivi la présentation, de nouvelles orientations se sont dessinées pour la suite de notre étude. Un rapport a d'ailleurs été produit à l'intention de la Direction de l'AFDS pour expliciter ces nouvelles orientations et les impacts sur les termes de notre contrat. (Jusqu'à présent nous n'avons pas reçu de feed-back formalisé pour nous confirmer dans cette nouvelle voie. Nous livrons ci-après le contenu résumé de ce rapport.

En effet, en raison des incertitudes sur l'avenir du système d'information central, son implantation, sa gestion, et la relation avec le projet de l'observatoire actuellement en gestation, il a été convenu d'accord parti :

- 1°) de s'orienter vers le scénario (numéro 2) d'architecture « BASES DE DONNES DISTRIBUEES », dans lequel il s'agira de mettre en œuvre pour chacune des entités, un serveur de base de données, pouvant être géré indépendamment, mais avec la même structure de données pour chacune des catégories informationnelles définies précédemment. Ce scénario a en effet l'avantage de permettre à chaque entité d'évoluer indépendamment, sans compromettre l'objectif de leur intégration à terme. Ce scénario serait donc explicité afin de définir une configuration minimale exigible pour chaque entité pour la future mise en réseau. Dans ce cas, le serveur central abritant la base de donnée centrale et le portail, serait relégué au second plan et à un futur prochain.
- 2°) les efforts doivent désormais être concentrés sur la mise en œuvre diligente et progressive des sous systèmes des entités d'une part, en y greffant les systèmes de gestion interne (particulièrement pour l'AFDS).
- 3°) de finaliser par conséquent de manière diligente la grille de concertation et d'identification des besoins informationnels, le principe retenu est d'y intégrer les résultats de l'étude sur les indicateurs synthétiques de l'AFDS actuellement en phase finale. [Notons que cette partie était en attente de prise en compte dans la grille de concertation, en raison de l'étude en cours, confiée à un consultant externe et non encore finalisé.]
- 4°) quant à la grille de perception, qui est le seul élément en attente d'être bouclé, elle va être différé à une date ultérieure, sachant que c'est elle qui précises la nature et la formes des vues à travers lesquelles les entités devront voir, les données consolidées et centralisées, issues de toutes les entités (cette base de données centrale étant reléguée au second plan).

- 5°) concernant la phase 3 de notre intervention, relative à la modélisation de la base de données, il a été suggéré de la shunter au profit des DAO des sous-systèmes, sachant que les spécifications de cette modélisation des données seraient intégrées dans les DAO afin de les faire prendre en charge par les prestataires chargés de la mise en œuvre de ces sous systèmes Bases de Données locales (architecture harmonisées). Rappelons que ces sous systèmes devront permettre de produire au niveau de chaque entité les informations dont celle-ci détient les prérogatives de production. En effet, les spécifications détaillées doivent permettre aux prestataires d'avoir des orientations précises sur les modalités de développement de ces systèmes.
- 4°) la dernière phase, enfin, relative à l'élaboration des DAO (dossiers d'appels d'offres) des différentes entités (équipements et SI), va être menée de manière à y intégrer les spécifications sur les modèles de données à mettre en œuvre (moins détaillées tout de même que celles qui était prévues dans la phase 3 initiale).

Dans cette opération, la priorité devrait être donnée à l'entité AFDS pour la sortie des DAO (équipements et SI). Même si cette décision est légitime, nous ne partageons pas pour autant, l'idée de choisir un seul prestataire pour la fourniture des équipements postes de travail et réseau d'une part et développement SI (SGBD) d'autre part. Nous recommandons de présenter ces DAO en deux lots distincts, n'excluant pas de fait les prestataires spécialisés dans l'un ou l'autre de ces deux domaines.

II 1^{ère} partie

PROTOCOLES D'ECHANGES

Nous avons, dans la première phase de la présente étude, fini par établir les prérogatives de chaque entité cadre du système d'information de lutte contre la pauvreté.

Ces réunions de concertation, portant sur les résultats du recensement des ressources et besoins informationnels ont permis les protocoles d'informations dont les termes sont présentés ici. Ces protocoles ont en effet pour objectif de définir les responsabilités et privilèges des usagers en matière d'entrée et de mise à jour des données dans la base de données du système central ainsi que les modalités de production locale de ces données (source, vecteur, format, périodicité de mise à jour etc.). et par conséquent de déterminer les fonctions principales dévolues aux sous-systèmes des entités respectives.

C'est à partir de ces prérogatives, que nous allons d'une part mesurer l'aptitude de chaque entité à pouvoir assurer cette production et introduction des données dans le système central à mettre en œuvre.

Les différentes réunions de concertation que nous avons supervisées ont donc abouti aux résultats suivants :

Pour chacune des six catégories d'informations retenues (indicateurs, projets, activités, intervenants, communautés et publications), il a été arrêté :

1°) la liste détaillée des rubriques qui la composent

2°) la désignation de l'entité en charge de la production de chacune de ces rubriques, le format, le niveau et la fréquence de sa production et les modalités de sa détermination. Pour la codification, certaines rubriques ont bénéficié d'une codification déjà opérationnelle à la DPS dans le cadre de la Live data Base (LDB), d'autres par contre qui ne sont pas actuellement codées (en lettres rouges dans le tableau) le seront suivant le même principe.

3°) Quant au niveau et la vue suivant lesquels chaque entité accédera aux différentes rubriques depuis la base de données centrale, le travail reste tout de même à être finalisé.

Nous dressons ici, les deux tableaux résultats de ces réunions de concertation :

le premier tableau définit les prérogatives de chaque entité quant aux modalités de fournir à la base de donnée centrale, les différentes rubriques des catégories informationnelles, de même que les formats dans lesquelles ces données seraient produites, leur périodicité, leur niveau de couverture (national, régional, départemental, etc..).

Ce tableau a été récemment enrichi des résultats d'une étude sur les indicateurs synthétiques spécifiques de l'AFDS. Ces éléments seront la base principale de son système interne de suivi.

ces elt. correspondent à 1 seul indicateur

1^{ere} Grille de concertation : (voir annexe 1)

Le second tableau, quant à lui, est une grille de perception ayant pour objectif de décliner la ou les vues, à travers lesquelles, chaque entité veut percevoir les données de la base dont elle a besoin (soit telles que produites, soit moyennant un retraitement, une consolidation etc.)

2^{eme} Grille de perception : (voir annexe 2)

Chaque entité aura à préciser ces vues et niveaux et à approuver et valider officiellement ces prérogatives.

Ce travail constituera la base de toute opération de mise en œuvre de bases de données locales dans les entités concernées. En effet, en raison de la mise en œuvre progressive des systèmes répartis dans les différentes entités, la logique applicative sera la même pour toutes les entités et ne va être définie qu'une seule fois, c'est à dire pour la première entité à déployer.

Les dossiers d'appels d'offres qui seront par conséquent confectionnés à la suite de ce document devront permettre de réaliser des bases de données s'appuyant principalement sur ces éléments décrits ici.

III 2^{ème} partie

ESQUISSE DE L'ARCHITECTURE TECHNIQUE DU SYSTEME

III.1 INTRODUCTION

L'étude préliminaire de faisabilité du projet de système d'information de lutte contre la pauvreté, a déjà permis de faire le choix parmi les différentes alternatives suivantes que sont :

- ⇒ La mise en œuvre d'une architecture avec un système centralisé sans disposition de sous-systèmes pour chaque entité.
- ⇒ La mise en œuvre d'une architecture avec des sous-systèmes interconnectés sans disposition d'un système central.
- ⇒ La mise en œuvre d'une architecture avec un sous système pour chaque entité et avec disposition système central,

L'option faite sur cette dernière configuration de base, de disposer d'un système central auquel sont connectés les sous systèmes respectifs des entités, a pour objectif de réaliser un couplage flexible, capable d'absorber les différences d'architecture technique entre entités tout en supportant les possibilités d'intégration, entre le système partagé et les systèmes de gestion internes.

III.2 LES SPECIFICATIONS FONCTIONNELLES

Cette ouverture du système d'information doit nous conduire à définir des architectures types de ces sous système, tenant compte du niveau d'informatisation de l'entité, du nombre et de la localisation géographique des utilisateurs, de l'ampleur de la base locale, sans oublier ses prérogatives dans la mise en œuvre de la base de données centrale. En effet, les différents pourvoyeurs d'informations ne seront pas toutes identiques, certains seront inévitablement dotés de réseaux locaux LAN avec serveurs en raison du nombre de postes de travail, d'autres par contre, seront dotés d'un nombre minimal de postes de travail (un à deux) en raison de la concentration, sur un nombre très limité de postes de travail, des informations à collecter.

L'architecture technique devra prendre en compte l'aspect intégration et harmonisation de l'ensemble des configurations locales existantes.

Les scénarios de configuration qui seront déclinés ici, doivent être perçus comme des modèles de référence qui vont servir de base à la définition et à l'implémentation des différents sous systèmes des entités. La véritable finalité réside dans l'harmonie et la compatibilité des sous systèmes déployés par rapport au système central, aussi bien dans les échanges que dans la gestion décentralisée des bases de données. En d'autres termes, ils devront offrir une plate-forme logistique harmonisée, à laquelle devront s'adapter tous les sous systèmes qui seront mis en œuvre graduellement, au fur et à mesure du développement du système et de l'intégration des entités opérant dans le cadre de la lutte contre la pauvreté.

3°) Sécurité, disponibilité et performance

Pour des raisons de disponibilité permanente de ces sous systèmes et du système central à terme, il sera mis en place un dispositif de duplication (back-up de sécurité), capable de prendre le relais en cas d'indisponibilité du serveur principal, et d'assurer ainsi une disponibilité permanente du système d'information.

Cette disponibilité devra être assurée par l'implantation de deux serveurs en parallèle, avec une procédure de réplication différée ou temps réel des mises à jour de la Base. Dans un premier temps, il sera surtout question de mettre en œuvre un système simple à gérer au niveau des entités.

4°) Applicatifs SGBD

Les applicatifs de gestion pour la gestion de la base de donnée seront au format WEB. L'ensemble des interfaces utilisateurs seront développés pour être utilisés via les navigateurs standards du marché.

Un accent particulier sera mis sur la sécurisation des transactions compte tenu des caractéristiques du réseau public internet à travers lequel s'effectueront les échanges, mais aussi et surtout, sur un fonctionnement optimisé dans cet environnement réseau à débit relativement faible (64 kbis/sec) dans certains cas de figure.

En terme de système de gestion de bases de données (SGBD), l'adoption du type relationnel permettra d'établir des liens plus importants entre la conception et la gestion physique des données. En outre c'est un moyen d'assurer plus facilement l'intégrité et la cohérence du système d'information et de faciliter par de là, les opérations de maintenance et de réadaptation du système d'information par rapport à son environnement et son évolution future.

Il devra en outre assurer des performances plus importantes par rapport aux autres types de SGBD. En effet, il apporte grâce à l'utilisation d'un support de langage de type SQL, une certaine facilité pour les utilisateurs, d'accéder aux données voulues et d'obtenir une forme d'indépendance par rapport aux informaticiens.

5°) Processus de mise en œuvre de l'architecture

La mise en œuvre de l'architecture globale du système d'information se fera selon le phasage suivant, retenu à l'issue de la revue à mi-parcours du projet Fond de Développement Social:

1^{ère} phase :

Elle concerne l'installation des sous systèmes relativement indépendants des entités avec en priorité celui de l'AFDS. Celle ci fera l'objet des premiers DAO (Dossiers d'appels d'offres) aussi bien pour la mise en place de l'architecture réseau local et postes serveurs et de travail, mais aussi le développement et la mise en œuvre des bases de données locales. Ces architectures seront déployées en harmonie avec l'architecture générale défini, et de manière à assurer leur intégration sans difficulté.

2^{ème} phase :

La mise en œuvre à terme du système central dont l'alimentation de la base de données centrale se fera depuis ces sous systèmes décentralisés.

Nous avons ci-après décliné les différentes composantes de cette architecture en deux scénarios distincts :

III.4 Déclinaison des scénarios d'architecture

Le système d'interconnexion entre les sous systèmes et le système centre

Les solutions groupeware et intranet sont aujourd'hui les outils de travail de groupe : messagerie, bases de données en particulier.

La solution GROUPEWARE INTEGREE, plus répandue sur le marché (Lotus Notes par exemple) est implémentée grâce à des outils très puissants avec de nombreux services et fonctions. Cependant, elle est très gourmande en ressources et puissance machine, mais particulièrement en coût. Elle reste de plus dépendant de solutions propriétaires évoluant suivant la stratégie commerciale des différents éditeurs.

La solution INTRANET par contre, a l'avantage d'être modulaire. En effet, l'on peut démarrer avec un nombre réduit d'acteurs et élargir graduellement les intervenants en fonction des besoins. Elle a aussi l'avantage d'engendrer un coût nettement moins onéreux et offre de plus une large panoplie de produits, tous compatibles en raison des standards du marché.

Contrairement à internet, où il est difficile de prévoir le nombre d'utilisateurs et d'intermédiaires, le réseau intranet, bien qu'utilisant la même technologie, est contrôlé et maîtrisé. Il est notamment dimensionné afin d'offrir des temps de réponses rapides dans les différentes applications qui y sont implémentées.

Enfin l'un des avantages notables d'intranet, est d'utiliser un client universel avec les navigateurs du marché (Netscape, Windows Explorer, etc.) mais plus particulièrement de permettre d'y implémenter des bases de données, des moteurs de recherche, des systèmes de production et de diffusion de documents et de faire appel à la technologie Java pour les applications évoluées.

La véritable problématique reste l'intégration de tous ces outils, leur administration et leur évolutivité dans le futur. Il faut en réalité des compétences informatiques et télécom spécifiques avérées pour les exploiter dans de bonnes conditions.

1. L'infrastructure

Plusieurs possibilités s'offrent dans le choix de l'infrastructure réseau, ils diffèrent cependant dans leurs technologies, les modalités de leur mise en œuvre et de leur exploitation, mais surtout les coûts de leur installation et de leur fonctionnement.

- **la liaison par le réseau public RTC**

Dans ce cas de figure, l'accès des entités se fait par l'intermédiaire du téléphone et d'un modem via RTC, sans chiffrement. Les inconvénients de cette méthode sont multiples.

- coût élevé des communications (régionales, nationales, voire internationales),
- faible débit, manque de sûreté (il est facile d'écouter ou de détourner une ligne téléphonique non chiffrée),
- difficulté d'accès (l'usage des modems est interdit ou impossible dans un nombre croissant d'administrations, pour des raisons de sécurité),
- peu pratique (il faut souvent redémarrer son ordinateur pour passer d'une connexion au réseau local à une connexion par modem).

Ces inconvénients risquent de freiner ou de marginaliser la pratique d'ouverture de l'intranet à d'autres intervenants.

- **la autres types de liaison**

D'autres possibilités existent cependant de coût relativement fixe (lignes et services loués ou achetés à coût fixe). Dès lors la comparaison de ces différentes liaisons ne peut être faite qu'avec des durées de communications et de liaisons connues.

Ainsi, les propositions des différents prestataires devront intégrer ces considérations et faire la meilleure offre possible. Les autres types de liaisons concernent :

- la liaison spécialisée (LS)

- le réseau IP SENTRANET de la Sonatel
- la liaison radioélectrique WIRELESS

2. les systèmes de sécurité

Internet étant par définition un réseau public, ouvert, il est indispensable de mettre en place à divers niveaux des outils de protection, notamment :

- des mots de passe d'accès
 - des clefs de chiffrement pour contrôler l'intégrité des données
 - des logiciels de filtrage (firewall) sur des machines dédiées, pour contrôler et autoriser les différents droits d'accès, ainsi que les zones d'accès et de transfert d'informations
- la passerelle
 - le pare-feu (firewall)
 - la gestion des utilisateurs et le système d'authentification

Les deux scénarios présentés ici, le sont dans l'objectif de permettre un choix judicieux en toutes connaissances de causes, de la part des décideurs. Nous avons voulu, à travers ces deux choix, présenter la possibilité d'avoir une architecture haut de gamme, incluant ce qu'il y'a de mieux dans l'état de l'art, mais aussi, l'autre possibilité d'implémenter une architecture simple, moins onéreuse, fonctionnelle et surtout évolutive vers le scénario 1 éventuellement.

Les objectifs communs aux deux scénarios :

Réaliser un ensemble de réseaux locaux interconnectés à un système central via un support de communication.

- faire évoluer les architectures réseau de manière souple et sécurisée

- Permettre l'accès à d'autres profils d'utilisateurs nomades ou distants mais isolés (ONG, etc...)
- Offrir divers supports de communication afin de diversifier les méthodes d'accès.
- Offrir un accès Internet sécurisé à l'ensemble du réseau d'acteurs

I.4.4 L'ARCHITECTURE GENERALE

Le schéma 1 (annexe 3) montre l'architecture globale du réseau. Les réseaux locaux distants accèdent aux systèmes centraux via un support de communication à définir. Les contraintes liées à la définition de ce support sont:

- le coût des redevances
- la fiabilité
- la disponibilité

Le réseau local LAN de chaque entité :

Au niveau de chacune des entités, il s'agira de mettre en œuvre un réseau de connexion des postes de travail de type intranet, afin de mettre en place déjà quelle que soit la taille de l'entité et le nombre de postes de travail, un instrument de communication principal interne mais de plus ouvert à l'extérieur (échanges avec le monde externe et en particulier au réseau public Internet).

C'est un mini réseau internet à l'échelle de l'entité. La configuration à mettre en œuvre aura l'avantage de fonctionner avec les mêmes normes, d'utiliser des lignes téléphoniques (RTC ou ISDN) sur lesquels seront connectés au plus simple, des modems et un accès à internet partagé.

L'avantage de cette configuration, très simple à implémenter, a un énorme avantage en terme de coût, et de plus elle utilise tous les outils, toutes les technologies existantes et livrés quasi gratuitement. La seule exigence est que le réseau exploite le protocole de communication IP (Internet Protocol).

Chaque réseau local sera de type Ethernet commuté (100 Mbits/s);

Des accès RNIS seront autorisés afin de permettre à tous types d'acteurs disposant des droits nécessaires d'accéder à la plateforme.

L'accès à internet sera partagé afin de diminuer les coûts d'exploitation.

- le serveur de DNS
- le serveur central de base de données
- le serveur principal de messagerie
- le serveur de fichier FTP
- le serveur WEB portail du système de lutte contre la pauvreté

II.4.4 LE SCENARIO 1 (schéma en annexe 4)

Cette architecture est celle d'un réseau privé virtuel (RPV ou VPN en anglais). C'est une liaison empruntant l'infrastructure de réseau public (internet) dont elle est isolée à l'aide d'un tunnel logique et, le plus souvent d'un procédé de chiffrement des données. L'idée est de faire transiter les données sur le réseau public internet qui implique des coûts de communication inférieurs, mais avec d'autres problèmes à résoudre, liés au transport, à la sécurité des données et à la qualité du service.

Cette configuration a l'avantage d'offrir un réseau de communication le plus extensible possible, en reliant de manière progressive des entités et intervenants du système de lutte contre la pauvreté. L'autre aspect non moins essentiel est sa capacité à fédérer des entités de taille différentes et même des intervenants de type itinérant, c'est à dire à l'aide d'un seul poste de travail indépendant.

Elle présente aussi une solution simple et évolutive avec diverses possibilités de connexion :

- En fonction des besoins et des moyens de l'entité, il peut être mis en œuvre des lignes de communication louées ou privées, mais les coûts sont vite ressentis en comparaison avec les autres possibilités ci-dessous
- Une autre possibilité est celle de l'utilisation du réseau téléphonique public et un serveur d'accès distant pour une

connexion via le réseau public internet (le plus simple est l'utilisation d'une ligne téléphonique et d'un modem).

- Cette liaison permanente entre le système central et les sous systèmes des différentes entités est réalisable selon les trois options suivantes :
 - Liaison LS
 - Réseau SENTRANET IP
 - WIRELESS
- Une base de données centrale, avec système de back-up automatique ou manuel
- Mise à jour sous forme transactionnelle à partir de l'ensemble des postes de travail du réseau.
- Le schéma en annexe 4 montre l'architecture détaillée du système central avec la répartition des serveurs.

La sécurité :

La sécurité sera gérée à plusieurs niveaux:

- au Niveau des accès: adressage IP privé et Firewall, Accès list au niveau des routeurs.
- au niveau des utilisateurs: Authentification et Autorisation gérée par un serveur radius
- filtrage d'URL et logiciel antivirus (qui sera géré à deux niveaux: passerelle et groupe de travail avec mise à jour automatique via le Web.
- des fonctionnalités de détection d'intrusion et d'optimisation de performances peuvent être introduites progressivement pour renforcer la sécurité
- d'autres fonctionnalités de sécurité de contenu peuvent aussi être introduites progressivement

L'administration du réseau

L'administration du réseau sera effectuée avec Cisco Works Windows.

L'administration d'un réseau de ce type peut être très complexe. C'est pour cette raison que nous proposons de familiariser d'abord l'administrateur aux outils simples qui lui permettront d'effectuer la plupart des tâches d'administration courantes.

La maîtrise d'un tel outil et les nouveaux besoins en d'administration justifierons l'acquisition d'un progiciel plus complet mais conforme aux réels besoins d'administration réseau.

Des tâches simples devront être au moins disponibles comme:

- La cartographie du réseau global commuté et distant
- Reconfiguration des équipements à distance
- Upgrade d'IOS (logiciel des équipements réseaux) à distance
- Prise en main à distance sur tous les équipements

Les règles d'exploitation du réseau devront être définies après la mise en place du réseau.

III.4.4 LE SCENARIO 2 (schéma en annexe 5)

La différence avec le scénario 1 tient sur :

- Le système d'interconnexion des sous systèmes du système central
- La décentralisation des bases de données et de leurs traitement dans les sous systèmes des entités
- La suppression des serveurs relais de messagerie dans les entités

En effet, dans ce scénario, c'est par le réseau internet de base que chaque entité accède au système central par l'intermédiaire de modems ou routeurs partagés.

Les bases de données sont décentralisées à travers les entités sources dans lesquelles le travail se fait en local, les mises à jour de la base de données centrale s'effectuant en batch à l'aide de transferts de fichiers de mise à jour (FTP) par internet.