Projet Appui aux Centres Régionaux d'Investissement et à la Promotion des Investissements

GBTI SEGIR Contract No. PCE-I-00-98-00015-00 TO 826

Rapport sur les aspects techniques liés à la mise en place du système d'information DCAE/CRI

novembre 2004

Soumis à:

Nadia Amrani, CTO
USAID Morocco

---

novembre 2004. *Ce rapport est produit par Morocco Trade and Development Services (MTDS) et Chemonics International. Les opinions émises n'engagent en rien l'USAID et/ou le gouvernement américain.*

Introduction

Lorsque un investisseur souhaite réaliser un projet d'investissement, il entre en contact avec les administrations pour accomplir un certain nombre de formalités administratives, soit via l'administration de tutelle qui couvre son secteur d'activité, soit par l'intermédiaire des Centres Régionaux d'Investissement : accès au foncier de l'État, conventions avec l'État, autorisations diverses, etc.

Aujourd'hui, pour l'investisseur, ces formalités administratives sont compliquées, chronophages et nécessitent de multiples allers-retours d'une administration à l'autre.

De plus, dès que l'on s'éloigne de Rabat, c'est-à-dire des Directions Centrales des administrations, les délais s'allongent.

Dans le cadre de la nouvelle orientation concernant la déconcentration des services de l'État, la création des CRI, via le guichet de l'investissement, a constitué une première étape pour rapprocher les services publics des investisseurs.

Aujourd'hui, avec le déploiement des accès au réseau Internet à travers le Royaume, notamment via l'opérateur public et son offre ADSL, il est possible d'imaginer des systèmes d'information permettant à la fois une nécessaire centralisation des données et une décentralisation des services, au plus près des investisseurs conformément à l'esprit de la Lettre Royale.

Le système imaginé n'est ni un réseau, ni un serveur, mais un système d'information comprenant des données et des documents, réunissant plusieurs services qui opèrent sur un même territoire et permettent les échanges d'informations et le travail coopératif en réseau.

La solution technique proposée repose sur l'utilisation du réseau Internet et la mise en place d'un réseau privé virtuel entre les partenaires.

1- Utilisation du réseau Internet

C'est donc un service qui utilise un réseau existant, Internet ; aussi la mise en place du système d'information (SI) n'est pas tributaire de la constitution d'un réseau ad hoc, mis en place localement entre services déconcentrés d'un même département ou d'une même région, mais se matérialise par la mise à disposition de l'application à laquelle les utilisateurs autorisés accèdent via leur navigateur Internet.

Cette solution est particulièrement flexible puisqu'elle n'impose aucun pré requis du point de vue de l'architecture des réseaux utilisés par les services déconcentrés pour accéder à Internet - qu'il s'agisse d'une connexion directe via un fournisseur d'accès à Internet ou d'une connexion au travers du réseau fédérateur de leur ministère de rattachement, pour ne citer que les cas les plus évidents.

Cette architecture peut également permettre aux partenaires de l'Etat, ne bénéficiant pas de l'accès à un réseau de deuxième niveau d'un ministère (par exemple les communes), de participer au SI.

Internet est un réseau public, c'est pourquoi afin de régler les problèmes liés à la sécurisation de l'accès aux données et à la vulnérabilité du réseau Internet, nous recommandons la mise en place d'un réseau privé virtuel (Virtual Private Network = VPN) entre tous les acteurs institutionnels (voire les professions intermédiaires dans un deuxième temps).

2- Mise en place d'un VPN

Un réseau privé virtuel (Virtual Private Network, VPN) crée un lien sécurisé ou « tunnel » empêchant tout accès non autorisé. Les données sont automatiquement chiffrées et envoyées via Internet au site distant où elles sont automatiquement déchiffrées.

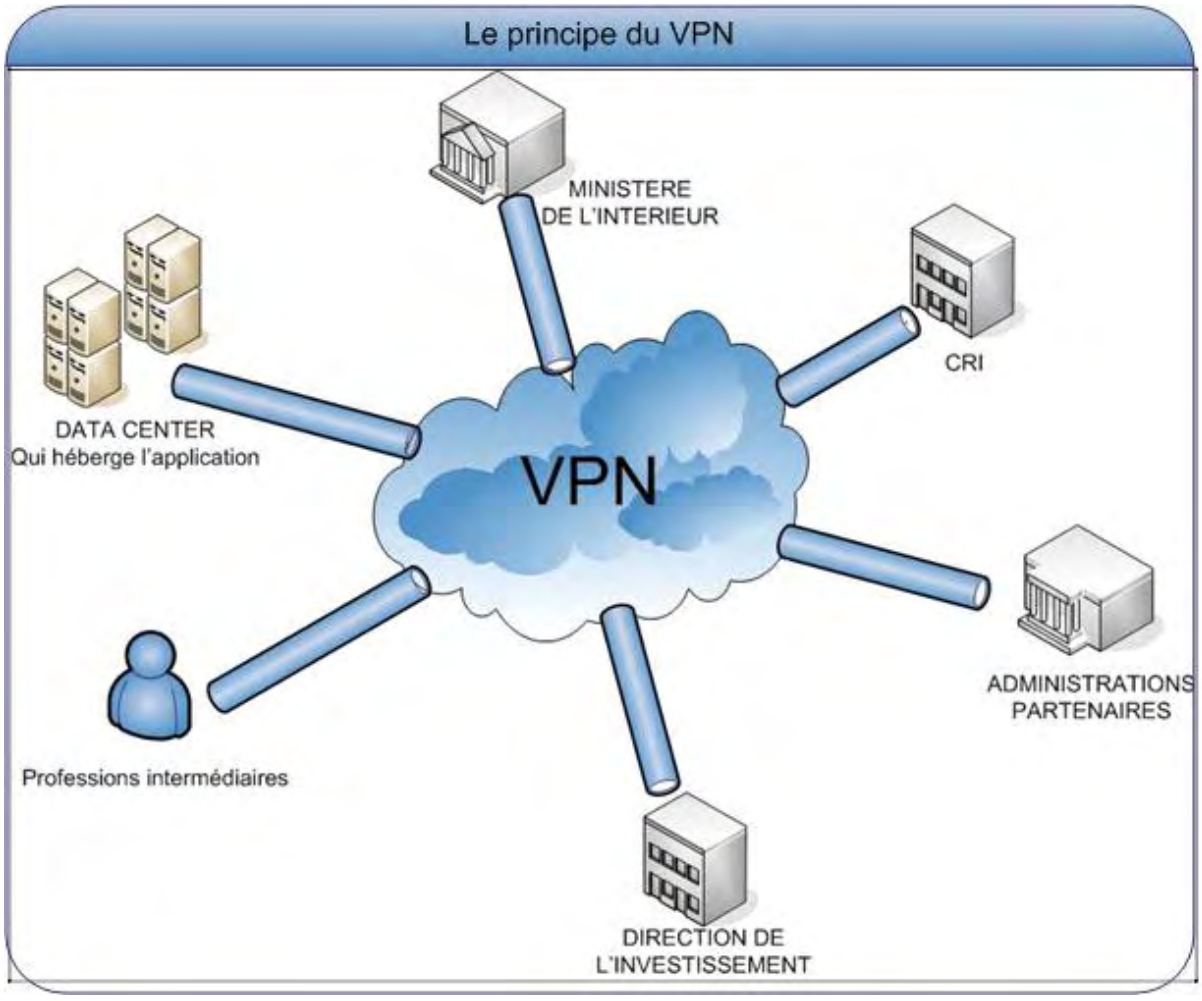
Il permet d'identifier les utilisateurs du SI-CRI de manière sûre et non ambiguë, pour mettre en oeuvre les contrôles d'accès en fonction des droits de chaque utilisateur, et permettre l'imputabilité des opérations effectuées.

L'accès au SI se fait au minimum par l'utilisation d'un login et d'un mot de passe. Ce contrôle d'accès se fait au niveau des individus et doit faire l'objet d'une gestion adéquate, afin d'éviter la prolifération de personnes pouvant accéder au SI.

Il permet un contrôle d'accès aux données puisqu'il n'autorise l'accès aux données stockées qu'aux personnes autorisées.

La plupart des CRI utilise un routeurs/pare-feu CISCO 515 qui permet la création d'un VPN facilement et à peu de frais.

Notons enfin que la mise en place d'un VPN permet aux CRI et aux autres partenaires connectés de partager d'autres ressources applicatives, par exemple pour la création d'entreprise.



3- Architecture technique de la plate forme

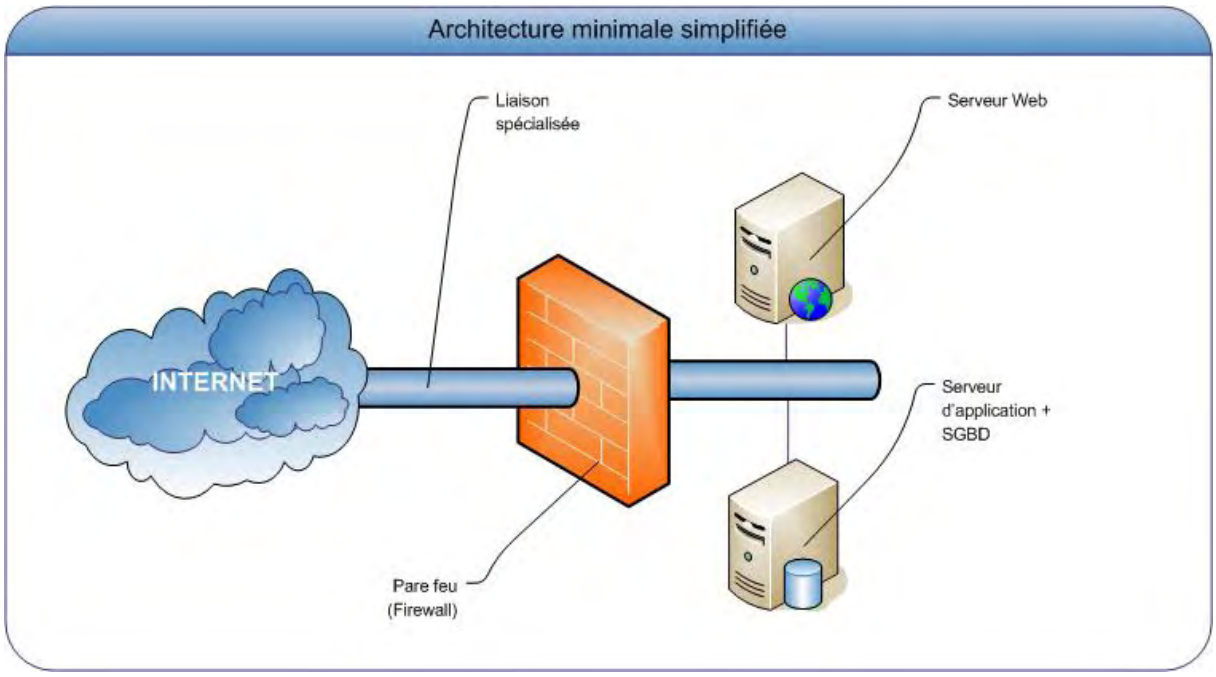
3.1 Solutions matérielles

Quelque soit l'option d'hébergement et pour des raisons évidentes de sécurité, nous recommandons l'acquisition de serveurs dédiés au système d'information.

L'architecture la plus sécuritaire et protégeant le mieux les données est une architecture étagée. Idéalement le serveur Web et la base de données doivent être sur des machines différentes.

Les données sont sur une machine inaccessible de l'extérieur et à laquelle seul le serveur Web a accès. Seul le serveur Web est accessible de l'extérieur, protégé par un pare-feu (firewall).

Un serveur « appliance » VPN/Firewall, machine avec des logiciels pré-installés, assure le rôle de pare-feu et gère le VPN.



3.2 Solution logicielle

Compte tenu de l'environnement existant, une solution 100% Microsoft semble la plus appropriée, même si la discussion sur les choix technologiques (du développement à la plate forme d'hébergement) doit, à ce stade, rester ouverte.

En tout état de cause, le système doit être extensible, pouvoir s'adapter à la demande et à la croissance, conférer à ses administrateurs beaucoup de contrôle et de souplesse, permettre aisément l'intégration de nouveaux modules et fonctionnalités.

4- Hébergement de la plate forme

L'hébergement consiste à la mise à disposition des ressources nécessaires pour permettre un fonctionnement continu du système nécessitant des ressources techniques et humaines.

Il existe différentes solutions pour l'hébergement des serveurs (nous ne parlons volontairement pas des hébergements mutualisés déconseillés pour des raisons de sécurité) :

- Héberger les serveurs au sein du service informatique de la DCAE
  - Avantages
    - Possibilité d'utiliser les ressources du Ministère (humaines et techniques)
  - Inconvénients
    - La continuité de service exigée impose des contraintes importantes : sécurité, équipements, astreintes du personnel, back-ups, etc.

- Héberger les serveurs au sein d'un centre d'hébergement
  - Avantages
    - Contractualiser les services attendus pour l'hébergement et notamment tous les aspects liés à la sécurité des échanges, la protection et le stockage des données.
    - Concentrer les ressources disponibles sur la gestion et la maintenance de l'applicatif : services aux utilisateurs, évolution logicielle.
    - Contractualiser l'engagement du prestataire sur la disponibilité des ressources.
  - Inconvénients
    - Risque inhérent à toute manipulation de données numérisées par un tiers : cession illicite de fichiers, piratage, etc.
    - Insécurité psychologique liée à la délocalisation physique des machines.

Notre avis :

Nous recommandons de confier l'hébergement et la gestion de la disponibilité du réseau et sa sécurité à un(des) prestataire(s) spécialisé(s) qui s'engage(nt) contractuellement sur des résultats : disponibilité du réseau, maintenance du VPN, etc. **Une attention toute particulière doit être apportée à la rédaction du contrat de service.**

Héberger le système chez un prestataire spécialisé n'empêche pas une gestion du système 100% à distance par une équipe du Ministère, notamment pour la gestion du contrôle d'accès aux services d'administration qui permet de n'autoriser les opérations d'administration du SGBD qu'aux utilisateurs disposant de droits particuliers.

- L'administration des données qui gère la structure des bases de données (création et modification de bases, de tables, de vues, d'index).
- L'administration de la sécurité (ou administration des utilisateurs) qui gère les utilisateurs, leurs méthodes d'authentification, leurs droits et qui effectue les audits de sécurité sur la base de données.

• L'administration technique qui effectue les tâches à caractère technique sur le serveur du SGBD, telles que lancement ou arrêt du service, sauvegarde/restauration de bases, optimisation de la structure de la base, supervision, monitoring…

Le contrôle d'accès aux services de gestion des utilisateurs est particulièrement important pour assurer la sécurité du SGBD.

5- La conservation des données

La fonction de conservation diffère de la sauvegarde informatique (ou " back up " qui lui, est assuré par l'administrateur système et dont la fréquence et le type doivent être précisés dans le contrat d'hébergement), dans le sens où les fichiers transférés sont sélectionnés et la durée de conservation des informations étendue.

Pour les dossiers d'investissement, il conviendra de s'interroger sur les délais de stockage et le traitement réservé aux dossiers traités, sachant que leur nombre ne peut qu'augmenter et que leur volume unitaire sera assez important (environ 1 Go par dossier).

Avant, peut être, le transfert de la responsabilité de l'archivage à un organisme ad hoc, le système d'information doit s'assurer de la conservation à long terme de ces données, ce qui correspond à sa mission dans la mesure où il s'engage à fournir un service sur la durée.

Soulignons seulement qu'il s'agit d'assurer que toutes les données soient disponibles, quelque soit le mode d'archivage choisi : machine dédiée, bande, etc. Plus intéressant serait, peut être, un système éloigné dédié à l'archivage (dans une institution ad hoc), accessible par réseau numérique en tout temps.

Il existe de multiples solutions d'archivage numérique, dont la problématique est transversale à toutes les administrations. A notre connaissance, il n'existe pas de normes marocaines en matière de conservation de données publiques. Un référentiel sur la conservation des données dans l'administration serait utile.

Conclusion

Le succès du projet repose sur un fonctionnement sans faille du système informatique et des télécommunications.

Le système d'information doit :

- **fonctionner 24/24, ce qui** implique que les ressources techniques, mais aussi humaines, soient dimensionnées pour permettre un service continu sauf cas de force majeure.
- **dans des conditions confortables d'utilisation,** c'est-à-dire avec une capacité de la bande passante bien dimensionnée pour suivre l'évolution du trafic,
- **et dans des conditions maximales de sécurité à tous les niveaux : accès, transfert, stockage.**

Le recours à un ou des prestataires spécialisés permettra d'une part de contractualiser la mise à disposition des ressources techniques (garantie d'une bonne exploitation de l'applicatif), d'autre part de concentrer les ressources sur l'évolution de l'applicatif et le service aux utilisateurs.

Annexes

1- Estimations budgétaires

1 KDH = 1000 DH

Investissements initiaux

Solution matérielle	
1 serveur dédié à l'applicatif et au SGBD	80 KDH
1 serveur Web	80 KDH
1 Firewall/VPN*	100 KDH
Solution logicielle	
1 SQLServer	80 KDH
Mise en place VPN, par 5 KDH par site	
Soit pour 20 sites,	100 KDH
Set up Hébergement	20 KDH
Imprévus	40 KDH
Total investissements pour 20 sites	**500 KDH**

Coûts annuels

Maintenance annuelle	
Maintenance constructeur VPN	15 KDH
Maintenance du réseau VPN*	150 KDH
Hébergement sécurisé	100 KDH
*Télécoms bande passante***	
En fonction du dimensionnement	de 100 à 400 KDH
Total coûts annuels	**de 375 à 675 KDH**

* Le coût associé à la gestion du VPN est à mutualiser avec les coûts associés aux autres applications partagées.

** La consommation de la bande passante varie en fonction du nombre d'utilisateurs et du volume des données qui transitent. Son coût est fixé par l'opérateur Maroc Télécom .

2- Le principe du VPN
http://www.commentcamarche.net/initiation/vpn.php3

3- Quelques prestataires marocains pour la gestion du VPN
www.ib-maroc.com
www.intelcom.ma
www.marocconnect.ma
www.mtds.com

4- Quelques hébergeurs marocains
www.menara.ma
www.wanadoopro.ma
www.mtds.com

5- Deux exemples d' hébergeurs internationaux ultra sécurisés:
http://www.thebunker.net/
www.servervault.com

6- Descriptif de deux plates formes d'hébergement conformes à l'état de l'art
http://www.easynet.fr/images/hebergement/fiche_hebergement.pdf
http://www.telehouse.net/Centre%20d%27h%E9bergementdef1.pdf

7- Article sur les enjeux de la conservation des données
www.ebsi.umontreal.ca/ebsi-enssib%5Cpdf%5Clebel.pdf