

**Une officine connectée, c'est pour vous, pharmacien, une vraie liberté : une ouverture sur le monde mais aussi la possibilité d'accéder aux données de l'officine depuis l'extérieur. Cet échange, créé au travers du réseau Internet, permet, en totale sécurité, d'utiliser des services très utiles dans l'activité professionnelle : la téléassistance, la téléformation, le télétravail.**

# L'OFFICINE À DISTANCE

## Téléassistance : une intervention directe d'experts

En cas de problème sur votre installation, la téléassistance permet une intervention à distance de votre SSII sur l'ensemble des postes informatiques. Avantages de ce type de service : la rapidité d'intervention, l'absence de coût téléphonique, l'utilisation d'outils spécifiques et performants pour établir un diagnostic précis.

## Téléformation : une formation « à la carte »

L'évolution de plus en plus rapide des technologies, les changements constants sur les logiciels et le matériel font naître un besoin croissant en formation. Quoi de plus adapté au métier d'officiel que la téléformation ? Ses points forts : une intervention sur le site, une formation individuelle et personnalisée ou collective, des disponibilités tenant compte de votre emploi du temps, un contenu adapté aux spécificités de votre officine (configuration logiciel et matériel, historique clients, etc).

## Télétravail : une efficacité permanente

Les nombreuses sollicitations et la présence des pharmaciens à diverses manifestations, congrès, etc, une activité professionnelle diversifiée (gestion de plusieurs officines, participation à la vie d'un groupement, d'un syndicat, etc)

rendent le télétravail particulièrement attractif. Par ailleurs, le travail quotidien du pharmacien comprend un certain nombre de tâches administratives qui n'ont pas besoin d'être traitées au sein même de l'officine. D'où l'intérêt, là encore, du télétravail.

Grâce à cette solution, vous pouvez consulter à distance l'exploitation de votre officine. Vous disposez d'un accès identique aux autres postes du réseau informatique et pouvez communiquer directement avec l'ensemble de vos collaborateurs.

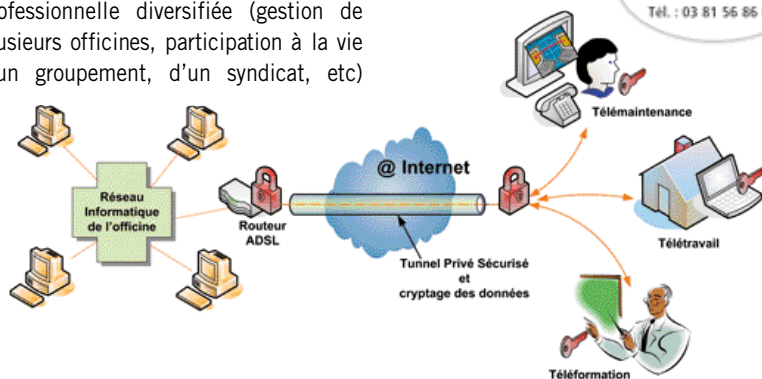
## Technologies de tunnelisation et sécurisation des échanges

Entre des points distants, il est nécessaire de créer des « liaisons informatiques », appelées tunnels. Ces tunnels utilisent généralement un réseau public (type Internet). Ils sont, de ce fait, souvent associés à une sécurisation des échanges par une authentification et un chiffrement. C'est la technologie la plus utilisée pour échanger des données de manière sécurisées au travers de réseaux qui ne le sont pas. L'ensemble des tunnels et des points de connexions distants constituent un réseau virtuel (VPN :

Virtual Private Network) permettant d'exploiter facilement des données ou applications distantes en toute sécurité.

On distingue deux catégories principales de sécurisation des tunnels. La première concerne la technologie PPTP (Point to Point Tunneling Protocol) ou son évolution L2TP (Layer 2 Tunneling Protocol). Elle correspond aux premiers protocoles capables de réaliser des tunnels ayant un minimum de sécurité par cryptage et authentification des données échangées. La seconde catégorie utilise des protocoles comme IPSec (IP Security Protocol) ou TLS (Transport Layer Security). Ceux-ci sont capables, en plus, de crypter le tunnel lui-même (par algorithme de chiffrement type RC4, 3DES) et d'identifier et authentifier leurs utilisateurs par certificats (type X509), ce qui leur assure un très haut niveau de sécurité.

TLS, un des protocoles les plus performants, reste le plus adapté aux accès distants sécurisés. Il constitue la meilleure solution à ce jour.



## règle d'or d'une liaison efficace

- ◊ **S'équiper d'une connexion haut débit d'au minimum 512 kb/s (1024 kb/s conseillé).**
- ◊ **Choisir un fournisseur d'accès « généraliste » dont la connexion autorise l'utilisation de ces services à distance.**
- ◊ **S'assurer de la mise en place d'une identification et d'une authentification forte utilisant des technologies de sécurisation des échanges. La sécurisation reste un domaine d'experts ou la « demi sécurité » n'existe pas.**