



LA SANTE MOBILE SUR iPHONE / SMARTPHONE



ketterthill

LABORATOIRES D'ANALYSES MÉDICALES

PLAN

Note Technique – Sécurité

- Système d'authentification
 - Authentification hors APN LuxGSM
 - Authentification 3G/APN
- Système de notification
 - Pré-requis
 - Sécurité et routage des notifications

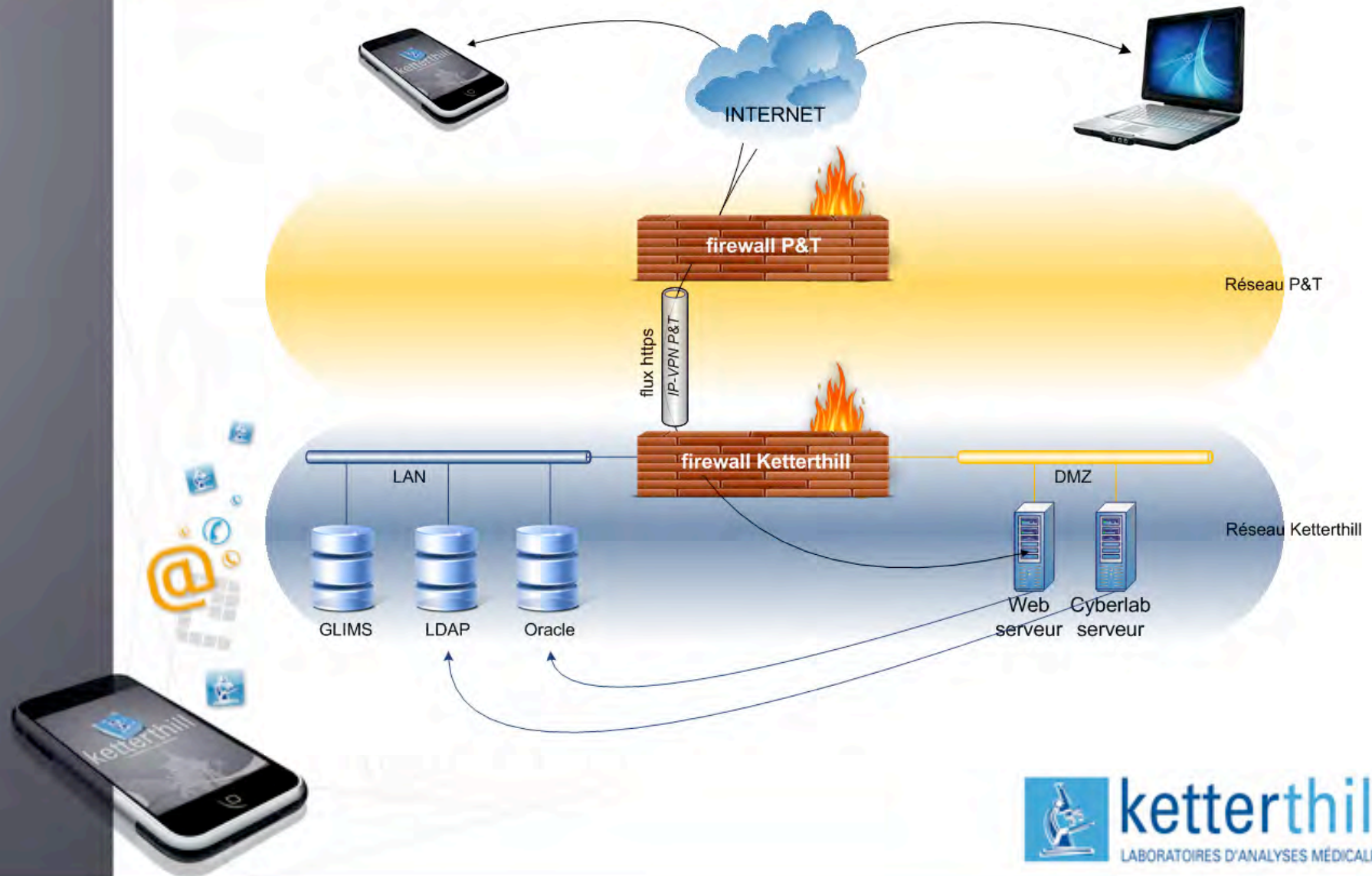


Systeme d'authentification

- Cyberlab[®] est un serveur de résultats développé par la société MIPS.
- L'accès est protégé par un couple d'identifiants Login/Password et l'utilisation du protocole HTTPS (ssl sur HTTP).
- Le serveur est identifié par un certificat public fourni par la société Equifax.
- Les utilisateurs sont authentifiés sur une base LDAP située dans le LAN.



Systeme d'authentification



Authentification hors APN

- Pré-requis
 - Un compte Cyberlab® (identifiants = Login/Password)
 - Une connexion Internet (ADSL, 3G ou Wifi)
- Accès au portail Ketterthill
 - Saisie des identifiants
 - Création d'une session sur le serveur de résultats
 - Accès automatique aux dossiers des patients
- À la fermeture de l'application
 - La session correspondante est détruite sur le serveur



Authentification hors APN

- Sécurité

- Les serveurs sont protégés d'Internet par deux firewalls indépendants et reposant sur des technologies différentes.
- Le firewall LKT (interne) possède un système de prévention d'intrusion (IPS).
- Seuls les protocoles standards sont autorisés par le firewall P&T (externe).
- Toutes les communications de l'extérieur vers les applications de la DMZ (hors serveur Web) sont cryptées (SSL).



Authentification 3G/APN

- Pré-requis
 - Un iPhone et un compte Cyberlab®
 - Un abonnement 3G
 - Pour les abonnés LuxGSM
 - Accès à l'APN privé Ketterthill
 - Adresse IP fixe attribuée dans l'APN
 - Lien unique : IP fixe ↔ identifiant médecin ↔ n° IMSI
 - Possibilité par la suite de ne pas ressaisir le Login
- Au démarrage de l'application
 - Identification du médecin (adresse IP et/ou identifiants)
 - Création d'une session sur le serveur de résultats
 - Accès automatique aux dossiers patients
 - Les droits d'accès sont contrôlés par le firewall et les identifiants
- À la fermeture de l'application
 - La session correspondante est détruite sur le serveur



Authentication 3G/APN



Systeme de Notifications

- Pré-requis

- Le médecin est abonné à Cyberlab® sur iPhone
- Le médecin a souscrit au système de notification pour les résultats perturbés

- Fonctionnement

- Basé sur le service de notification « Push Message » d'Apple (APNS)



Systeme de Notifications



1. Le serveur (Provider) communique en **permanence** par un canal **sécurisé** (certificats à clés publiques) avec les serveurs de l'APNS. Il fournit quand c'est nécessaire un message contenant le couple (information/token).
2. Le token est unique (fourni par l'APNS) et correspond à un iPhone déterminé.
3. Tout iPhone (allumé et connecté à internet) est **authentifié** et connecté en permanence de façon **cryptée** (certificats à clés publiques) sur l'APNS. Il récupère des notifications pour les applications installées et spécifiées par l'utilisateur.
4. En cas de notification, l'application installée sur l'iPhone se connecte sur le serveur de notification concerné pour récupérer les messages.



Systeme de Notifications

Remarques

Une notification est une relation univoque entre le serveur de notification de l'application et l'iPhone concerné.

Le message de notification ne contient aucune information sur le patient.

Si l'iPhone est éteint ou hors réseau, le message de notification est stocké sur l'APNS.

Les différents canaux de communication (Serveur/APNS, APNS/iPhone et iPhone/Serveur) utilisent le protocole TLS avec des certificats signés. Les différents certificats et le CA (Autorité de Certification) sont fournis par l'APNS.



Conclusion

La sécurité du projet est garantie par

- L'utilisation de protocoles standards (HTTPS, TLS)
- L'utilisation d'un reverse-proxy dans la DMZ
- L'utilisation d'un double firewall
 - Firewall P&T en entrée de réseau
 - Firewall interne entre le réseau P&T, la DMZ et le LAN
 - + Système de prévention d'intrusion
- Le respect des procédures des applications utilisées (APNS)
- L'utilisation d'un APN spécifique pour l'authentification en 3G
- La nécessité de saisir à chaque fois ses identifiants
- La formation des utilisateurs finaux (verrouillage du téléphone)
- La veille technologique



Compatible iPad

En plus des fonctionnalités actuelles, l'application « Ketterthill » sur iPad permettra au médecin d'accéder à la prescription connectée depuis un support mobile

