USE CASE

SÉCURISER DES DOSSIERS MÉDICAUX

Cas d'un centre hospitalier : protéger les dossiers des patients, consultés depuis un parc de terminaux légers

EXIGENCES

Un décret impose que seuls les titulaires d'une carte de Professionnel de Santé puissent accéder aux dossiers médicaux. L'établissement souhaite aller plus loin et **protéger également les données contre le vol et les fuites, et donc protéger la donnée elle-même.**

La solution doit s'adapter au système d'information, composé de **45 serveurs Windows, des SAN, deux annuaires AD, 20 serveurs Citrix™ et plusieurs centaines de terminaux légers Wyse.**

Les contraintes de performance et de tenue en charge sont primordiales. En effet, les fermes de serveurs Citrix™ **hébergent les sessions des utilisateurs en simultané :** les terminaux légers Wyse, installés dans tout l'hôpital, **disposent d'un lecteur de carte à micro-processeur** pour authentifier le personnel soignant et lui permettre d'accéder aux dossiers médicaux des patients. La solution doit **cloisonner les données dans un environnement multi-utilisateurs,** selon la fonction et le rôle de l'individu (personnel soignant ou administratif). Le produit doit être indépendant de la technologie de stockage.

SOLUTION

Le client a ainsi sélectionné le produit **ZONECENTRAL** pour :

+ **Sa compatibilité avec l'architecture Citrix™ :** malgré des pics de montée en charge jusqu'à 120 utilisateurs simultanés dans une même zone de chiffrement, la solution est parfaitement stable ;

+ Sa réponse à **l'impératif de chiffrement multi-utilisateurs.**

EXPÉRIENCE

Une série de procédures a été mise en place afin de **garantir la séparation des fonctions :**

+ La DSI gère les certificats ;

+ Les métiers gèrent le droit d'en connaître ;

+ Le responsable informatique a accès aux zones de chiffrement pour leur maintenance, mais n'a pas accès aux contenus lisibles qu'elles contiennent.

AVANTAGES

L'établissement peut non seulement respecter l'obligation de contrôle d'accès aux données médicales, mais aussi **parfaire la séparation des rôles grâce au chiffrement :** les données ne sont accessibles qu'au personnel habilité et leur manipulation est encadrée.

Le recouvrement, étape cruciale, est aussi très encadré : **aucun administrateur ne peut déchiffrer seul les données.** Il est nécessaire pour cela d'impliquer la DSI (pour l'accès aux données de recouvrement), le service médical (pour le code PIN de la carte de recouvrement) ainsi que la Direction (détenteur de la carte de recouvrement, mais pas du code associé).

ZONECENTRAL

PRIMX
MAKE ENCRYPTION HAPPEN

business@primx.eu – Tél. : 01 40 95 24 80
Siège social : 18 Rue du Général Mouton-Duvernet, 69003 Lyon / Direction commerciale : 21 Rue Camille Desmoulins, 92130 Issy-les-Moulineaux
www.primx.eu