USE CASE

ZONECENTRAL

HEALTH

SECURING MEDICAL RECORDS

Case of a hospital: protecting patient files, consulted using a fleet of thin clients

REQUIREMENTS

According to law, only holders of a health professional card can access medical data. The hospital wanted to go further in this regard and **also protect against data theft and leakage, while protecting the data itself.**

The solution needs to adapt to the information system, comprising **45 Windows servers, SANs, two AD directories, 20 Citrix™ servers and several hundred Wyse thin clients.**

The performance constraints and load performance are of paramount importance. The Citrix™ server clusters **host user sessions simultaneously** and the Wyse thin clients, installed throughout the hospital, **have a smartcard reader** to authenticate caregivers and give them access to patients' medical records. The solution must **partition the data in a multi-user environment**, according to the function and role of the individual (caregivers or administrative personnel). The product must be independent of the storage technology.

SOLUTION

The customer therefore selected the **ZONECENTRAL** product for:

+ **Its compatibility with the Citrix™ architecture:** despite load peaks of up to 120 simultaneous users in the same encryption zone, the solution is perfectly stable;
+ Its response to **the multi-user encryption imperative.**

EXPERIENCE

A series of procedures were put in place to **ensure the separation of functions:**

+ The CIO manages the certificates.;
+ The business lines manage the right-to-know;
+ The IT manager can access the encryption zones for their maintenance, but cannot access the readable content they contain.

BENEFITS

Not only can the establishment comply with the obligation to control access to medical data, but it can also **perfectly separate the roles thanks to encryption:** the data is only accessible to authorised personnel and the handling of the data is strictly controlled.

Recovery, a crucial stage, is also strictly controlled: **no administrator alone can decrypt the data.**

To do so, it is necessary to involve the CIO (to access recovery data), the medical department (which holds the PIN code of the recovery card) and Management (which holds the recovery card but not the associated code).

2023.06

PRIMX
MAKE ENCRYPTION HAPPEN

business@primx.eu - Tel: +33 (0)1 40 95 24 80
Head Office : 18 Rue du Général Mouton-Duvernet, 69003 Lyon / Sales Department : 21 Rue Camille Desmoulins, 92130 Issy-les-Moulineaux
www.primx.eu