L'Expertise du Coffre-fort Bancaire au Service du Dossier Patient

du Secret Bancaire au Secret Médical

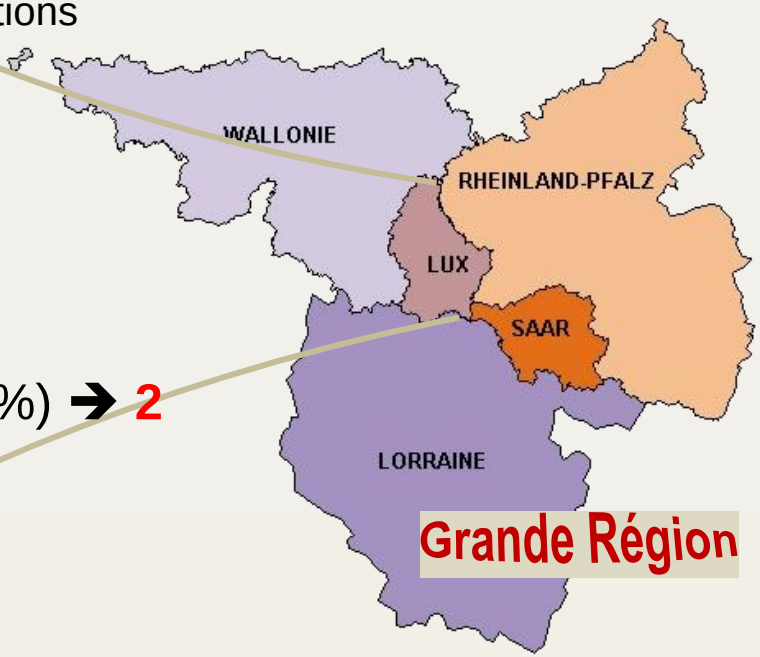
ebrc
TRUSTED DATACENTRE, CLOUD & MANAGED SERVICES

AGENCE eSanté LUXEMBOURG

GS Days 18 mars 2014

Secteur des Soins à Luxembourg

- Habitants **525.000**
- Résidents ➔ **44% = 170** nationalités
- Frontaliers ➔**155.000**
- Hôpitaux majeurs ➔ **5**
- Hôpitaux régionaux ➔ **5**
- Médecins (inclus dentistes & physiothérapeutes) ➔ **2.200**
  - Majorité de médecins libéraux y compris en institutions
- Professionnels secteur hospitalier ➔ **4.200**
- Pharmacies ➔ **100** (**445** pharmaciens)
- Laboratoires
  - National ➔ **1**
  - Groupes de laboratoires privés ➔ **3**
  - Hospitaliers ➔ **10**
- Prestataires de soins à domicile (couverture 97%) ➔ **2**
- Institutions de soins de longue durée ➔ **60**
- Recherche – Epidémiologie – Statistiques
- Grande Région + BENELUX ➔ **15 M** habitants



- **Le cadre du projet Dossier de Soins Partagé**
- La sécurité du Dossier de Soins Partagé

Enjeux et Contexte du Projet eSanté

2006 - Plan d'action eSanté

- ***Qualité*** *et* ***performance*** *des soins de santé*
  ➔ <u>disponibilité</u> des données médicales

- *Maîtrise de* ***l'évolution des dépenses***
  ➔ <u>partage</u> des informations

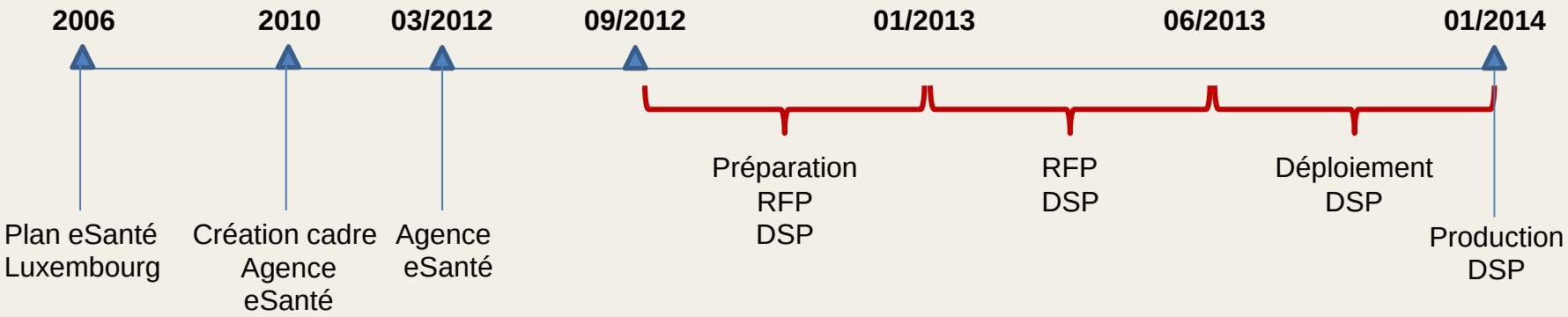
- ***Transparence sur les coûts*** *des prestations*
  ➔ <u>promotion</u> des alternatives de traitement

- ***Interopérabilité*** *du système de santé luxembourgeois*
  ➔ orienté <u>réseau européen</u>

2010 - Définition de la mission première de l'Agence eSanté

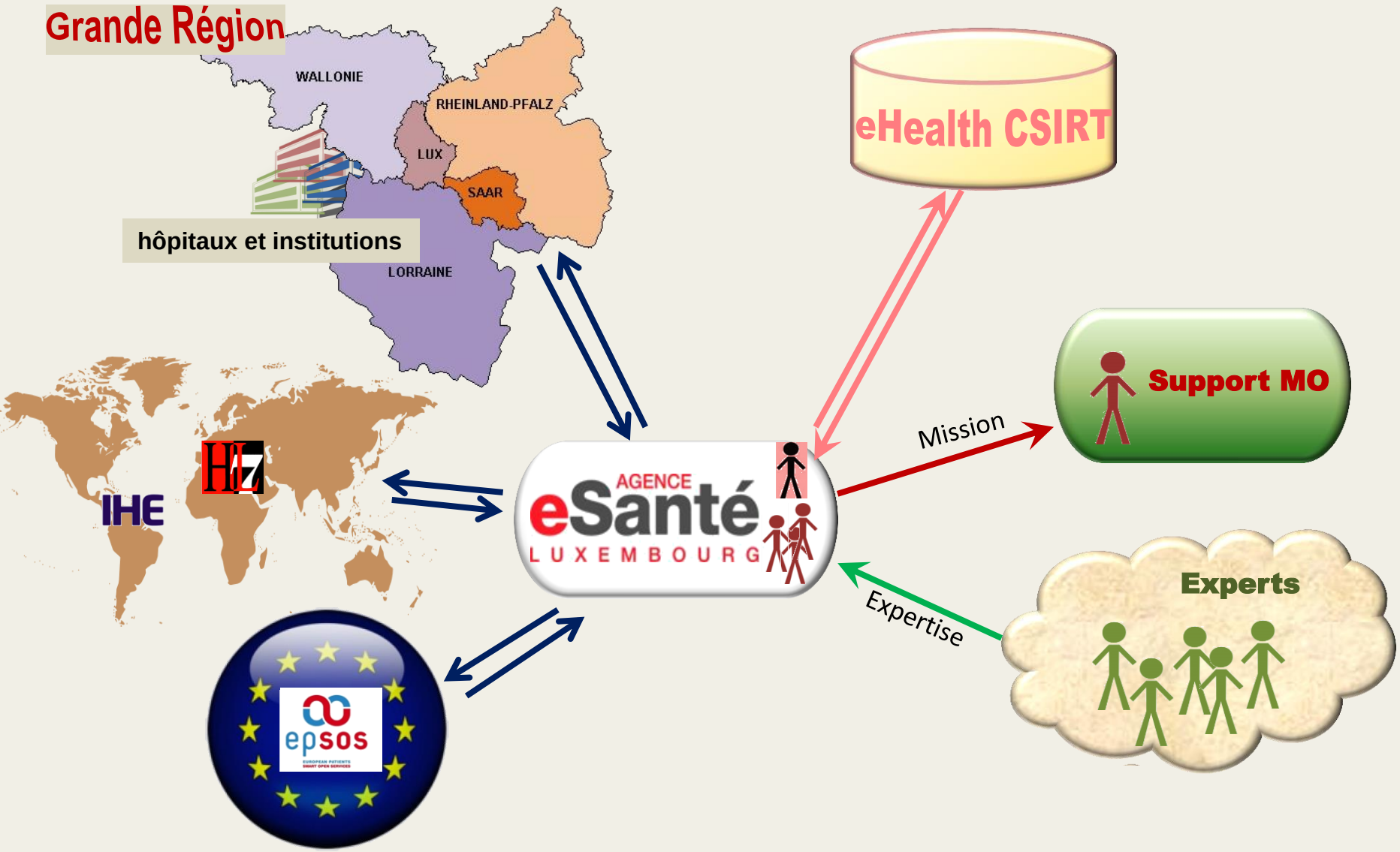
- *Mise en œuvre de la* ***plateforme d'interopérabilité:*** partage et échange des données
- *Politique de* ***gestion*** *et de* ***traitement*** *des données*
- *Solutions pour assurer la* ***confidentialité*** *et la* ***sécurité*** *des données*

L’Agence eSanté



Priorités ➔ Schéma Directeur
➔ Plateforme eSanté → DSP

Centre d'un écosystème Healthcare

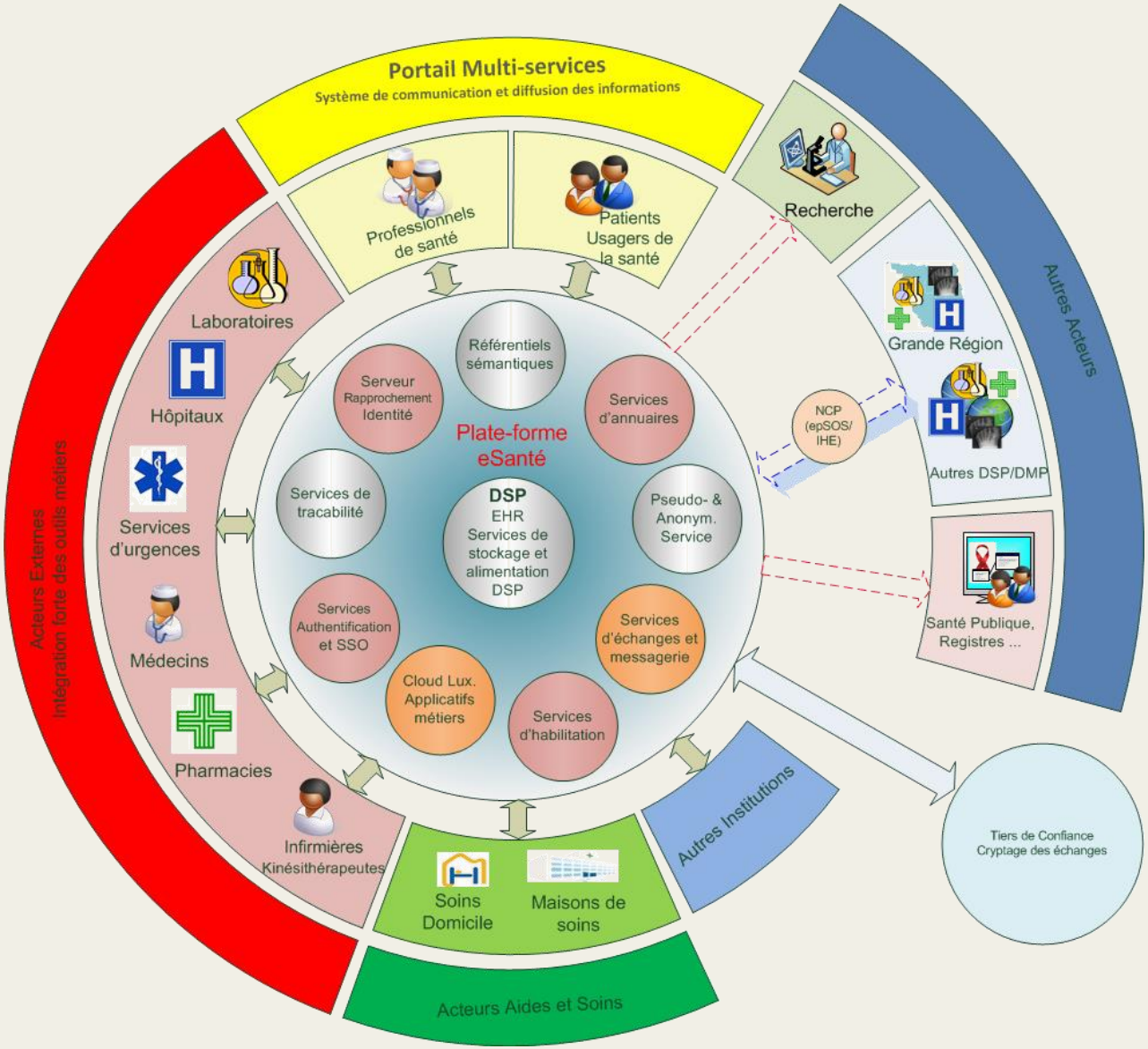


Plateforme eSanté – Adoption du DSP

- Freins au déploiement, peur de la nouveauté induite par
  - le changement de Technologie pour un modèle numérique
  - des Processus et des Usages

- Facteurs clefs de succès pour un modèle sécurisé et rassurant
  - Identification des usages
  - Accompagnement des utilisateurs

Services Offerts par la Plateforme eSanté



Partenaires du DSP

SQLI GROUP

Expert en solutions de eSanté

- Expérience unique dans la mise en œuvre de plateformes régionales
- Forte expertise en interopérabilité IHE/HL7
- Une expérience dans la gestion, la production, la collaboration médicale, la télé médecine, les PACS, RIS, laboratoires et EMR

Application

ebrc
TRUSTED DATACENTRE, CLOUD & MANAGED SERVICES

Leader Européen pour la gestion des informations sensibles

- Offre hébergement Cloud avec services managés au sein de deux Data Centres certifiés Tier IV
- Expertise en sécurité des plateformes et consolidation des processus

Infrastructure

accenture
High performance. Delivered.

Spécialiste ICT et acteur majeur, expert dans le secteur Santé

tudor
PUBLIC RESEARCH CENTRE HENRI TUDOR

Centre de recherche
Expert dans le domaine de l'interopérabilité sémantique et technique

regify®
your mail matters

Solution de cryptage pour assurer la transmission des messages

Accréditation des acteurs de support en secteur bancaire

- Cadre légal de protection des données ➔ CNPD

- Cadre légal du secteur financier luxembourgeois
  ➔ règles de fonctionnement et de protection secteur bancaire avec surveillance de la CSSF (autorité de contrôle)

- Les prestataires en environnement bancaire sont
  - légalement responsables au même titre qu'un banquier: **personnel** et **sociétal**
  - opérés dans le respect de **règles opérationnelles** strictes
  - **surveillés** par la CSSF : audit, reporting

- Le cadre du projet de Dossier de Soins Partagé
- **La sécurité du Dossier de Soins Partagé**

Urbanisation du SI au Service de la Sécurité

Sécurisation de la Plateforme eSanté par les 4 couches du SI

- **Couche Métier**
  - Objectifs globaux de la plateforme y inclus objectifs de sécurité
  - Objectifs et stratégie du DSP → Patient Centric ➔ Contrôle et rôle pivot du patient
  - Organisation des processus et des activités dans un cadre prioritaire d'identito vigilance
- **Couche Fonctionnelle**
  - Les services et les acteurs: identification et définition des règles,
  - Elaboration du référentiel du SI : processus, services métiers, composantes et flux normés (IHE)
  - La pièce angulaire, la matrice d'habilitation, identification des rôles et profils
- **Couche Applicative**
  - Architecture de services : articulations et composantes logicielles
  - SOA, puissance et sécurité du modèle SSO: les annuaires MPI et HPD
  - L'interopérabilité au cœur de l'intégration
  - Le cryptage des échanges d'information
  - Tiering applicatif et segmentation réseau
  - La sécurisation des données : disponibilité, pérennité, intégrité, auditabilité et traçabilité des informations
  - La sécurisation des fonctionnalités: redondance et haute disponibilité
- **Couche Infrastructure**
  - Infrastructure de type Community Cloud eSanté en mode dual site (Tier IV)
  - Les opérations: annuaire, traçabilité, consistance
  - Architecture globale établie sur base des référentiels CSA et PCI DSS: segmentation, règles, accès, …

Démarche sécuritaire

Analyse des risques

Définition d'une politique de sécurité

Application de la politique de sécurité

Evaluation de la politique de sécurité

Un édifice bâti pour la Sécurité

Trusted Advisory Services | Trusted Managed Services | Trusted Cloud Europe | Trusted Security Europe | Trusted Resilience Services | Trusted Data Centre Services

Niveau Application

- Règles d'interopérabilité
- Architecture SOA

IHE HL7

Trusted Cloud Europe

- Community Cloud eSanté

CSA cloud security alliance | PCI DSS COMPLIANT CERTIFIED

Data Centre

- Redondance - Dual site
- Tier IV Certifiés

TIER IV DESIGN – EBRC – Luxembourg Resilience Centre West – UPTIME INSTITUTE CERTIFIED

TIER IV FACILITY – ebrc – Luxembourg Resilience Centre South – UPTIME INSTITUTE CERTIFIED

ISO 27005 | ISO 20000:2011 | ISO/IEC 27001:2005

Advisory Services | **Managed Services** | **Security Services**

OSSTMM | OWASP

ISO 9001 | PRINCE2 | ITIL

Politique de Sécurité

ENTREPRISE SOCIALEMENT RESPONSABLE

Conformité aux lois et règlements

Schéma Directeur → Objectifs du DSP

Opérations avec SLA 24/7

Trusted eSanté - Services DSP

Sécurité globale de la plateforme

- **Confidentialité**
  - Accès portail ➔ matrice d'habilitation : rôles/accès
  - Accès patient ➔ fonctionnalités via SSO
  - Accès professionnel ➔ fonctionnalités via SSO **+** Certificat
  - Accès opérations ➔ VLAN + AD + Token authentification forte
  - Échanges ➔ cryptage et signature applications et acteurs (SSL)
  - Personnes ➔ EBRC Tiers de Confiance (règles sociétales et personnelles CSSF)

- **Intégrité et Disponibilité**
  - Redondance ➔ application
    ➔ data base
    ➔ infrastructure : Serveurs + Storage
    ➔ sites des data centres

- **Preuve - Non répudiation**
  - Traçabilité ➔ opérations **+** utilisation **+** messagerie (horodatage)

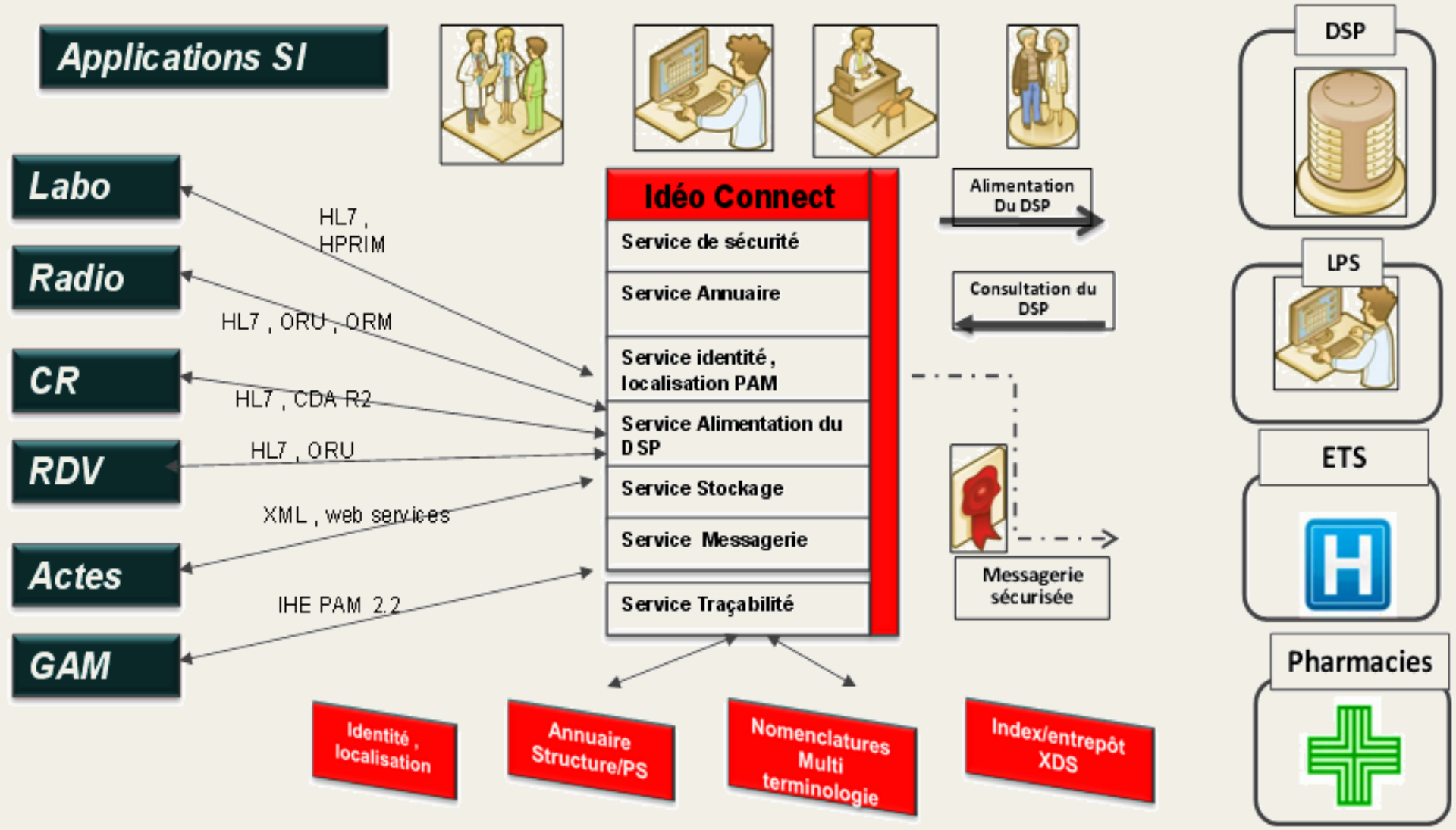
Contrôle de la sécurité

- **Architecture et composants**: outils de contrôle et de surveillance dynamique et préventive avec traçabilité des événements
- **Application** ➔ conforme aux normes IHE/HL7 avec traçabilité (ATNA)
  ➔ Web Services certifiés

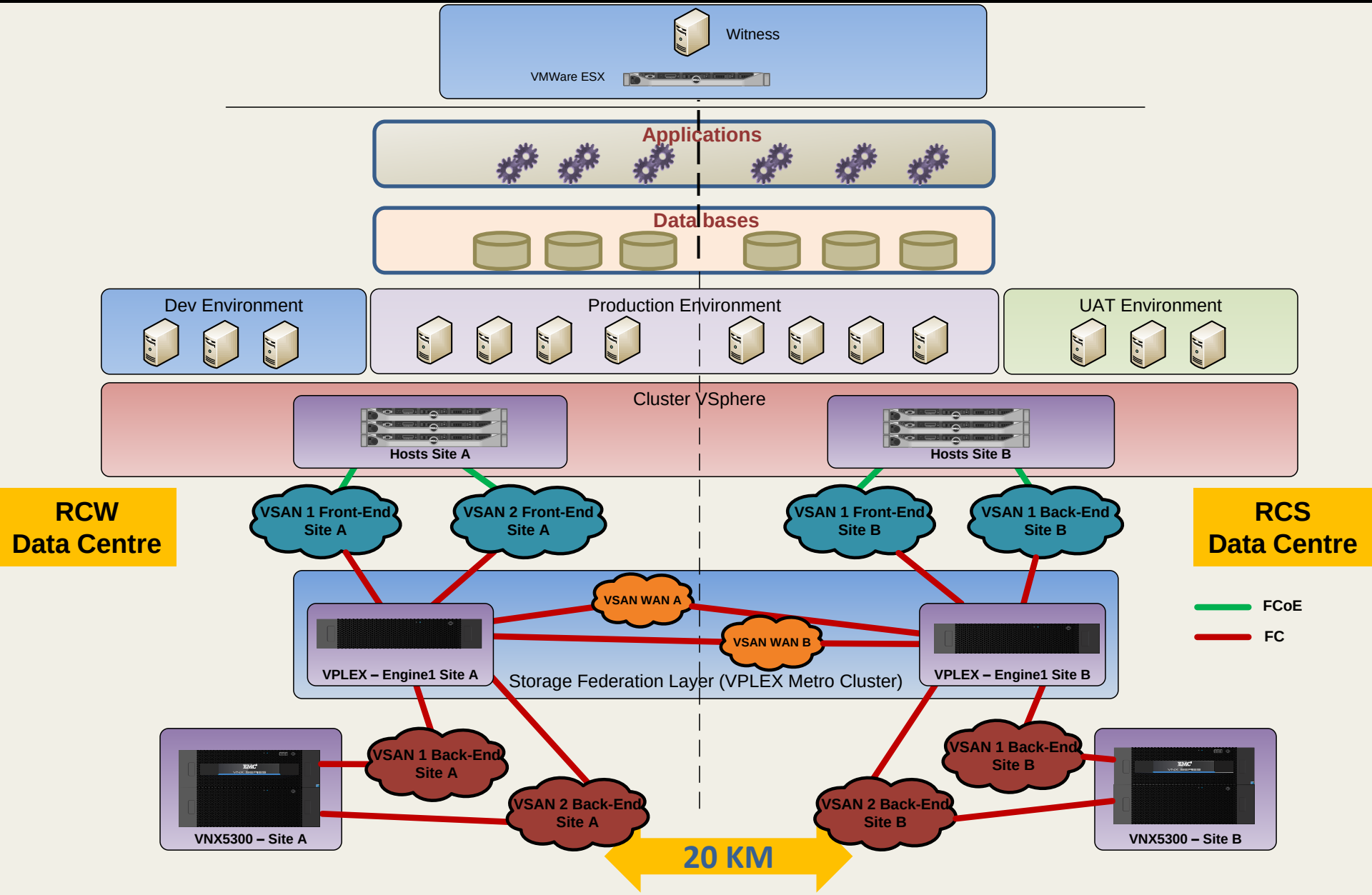
Validation de la sécurité

- **Audits récurrents**: assurés par des ingénieurs certifiés et selon les méthodes OWASP

Plateforme eSanté – le DSP



Objectif Redondance des Couches



Contrôle des flux, annuaires et traçabilité des accès

- **Contrôle des flux**

RBAC par environnement + PW Management
RHEL IPA ➔ cible unique : PROD ou PRE PROD ou INTEGRATION
VPN ➔ adapté à la cible site2site / client2site

- **1 fonction = 1 annuaire**

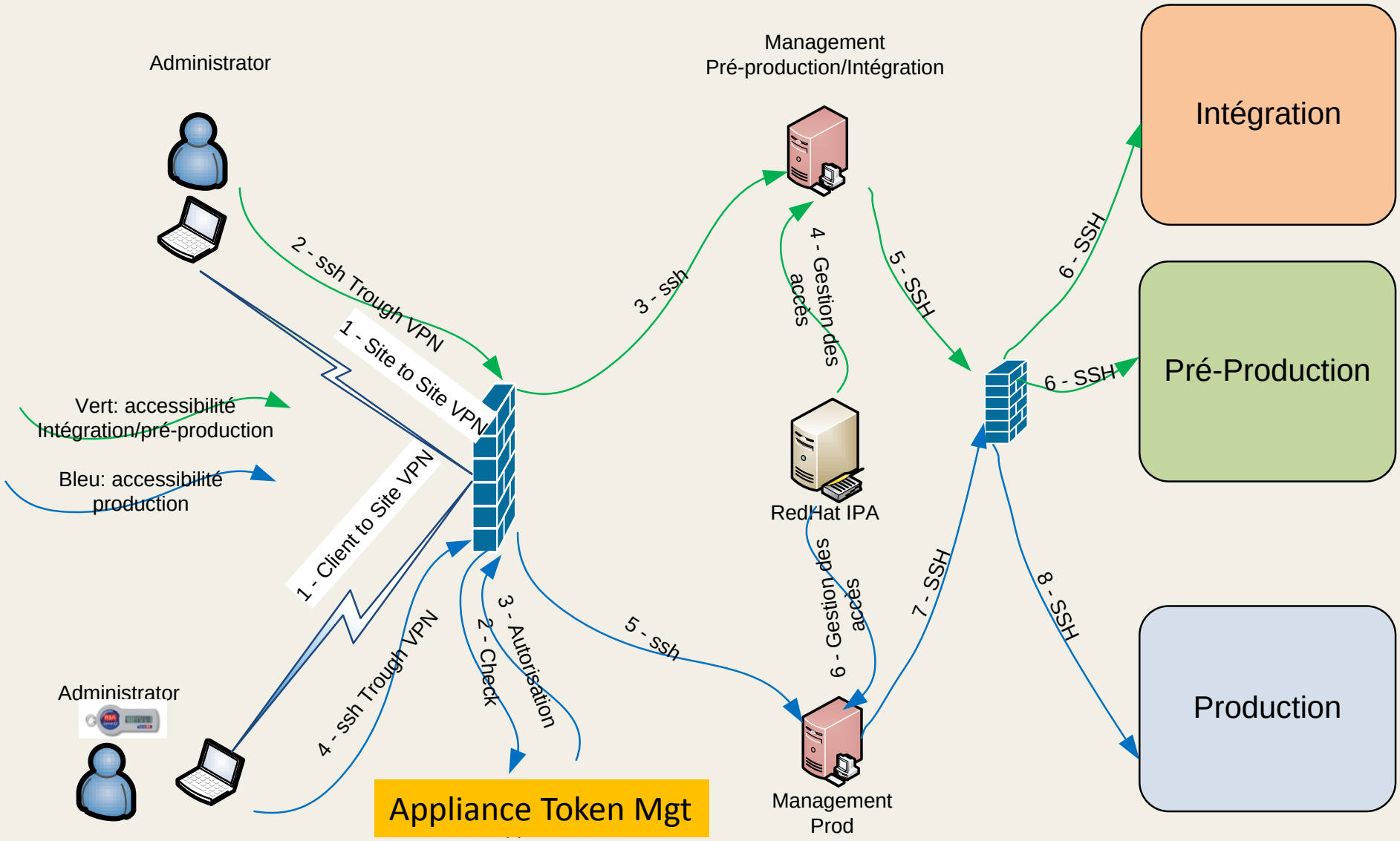
  - *Accès régulé par SSO et SSL*
    - Professionnels de Santé ➔ annuaire HPD et authentification forte via certificat
    - Patients ➔ annuaire MPI

  - *Accès régulé par RHEL IPA et VPN*
    - Exploitants ➔ annuaire LDAP et authentification forte via token

- **1 fonction = 1 trace spécifique**

– Utilisateurs ➔ entrepôt d'audit XDS transactions liées au DSP
– Exploitants ➔ traces systèmes Syslog NG

Accès d'administration technique



Trusted eSanté Services
Maîtrise des risques

Analyse des risques

- Revue cyclique
  - Probabilité d'occurrence ou existence (incident…)
  - Impact potentiel en cas d'occurrence
  - Première évaluation des hypothèses et alternatives de neutralisation

Classification des risques

- Hiérarchisation vs degré d'impact
  - potentiel ou réel
  - isolé ou générateur d'un effet cascade
  - bloquant ou non bloquant
  - poids du risque vs conséquences

Traitement des risques

- Détermination des mesures
  - Inventaire des hypothèses de correction et de neutralisation
  - Evaluation et choix des mesures correctives à appliquer
- Communication
  - Information et implication des personnes/comités en rapport avec la classe (Low→high) ➔ Dispositif de gestion de crise
- Application des mesures
- Clôture des actions liées au risque

Habilitation des accès au DSP

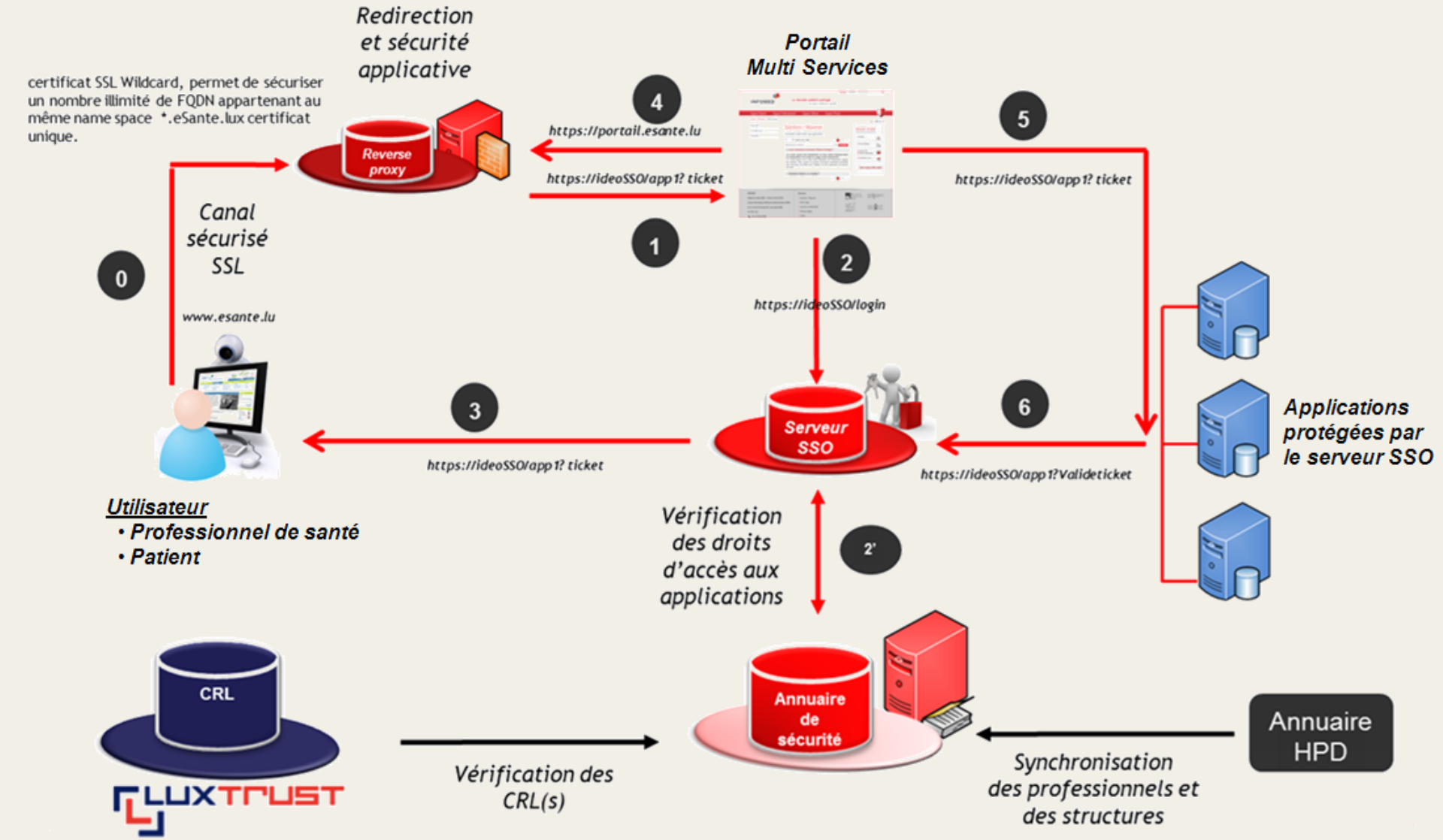
Identification et authentification de l'utilisateur

Identification et existence du DSP

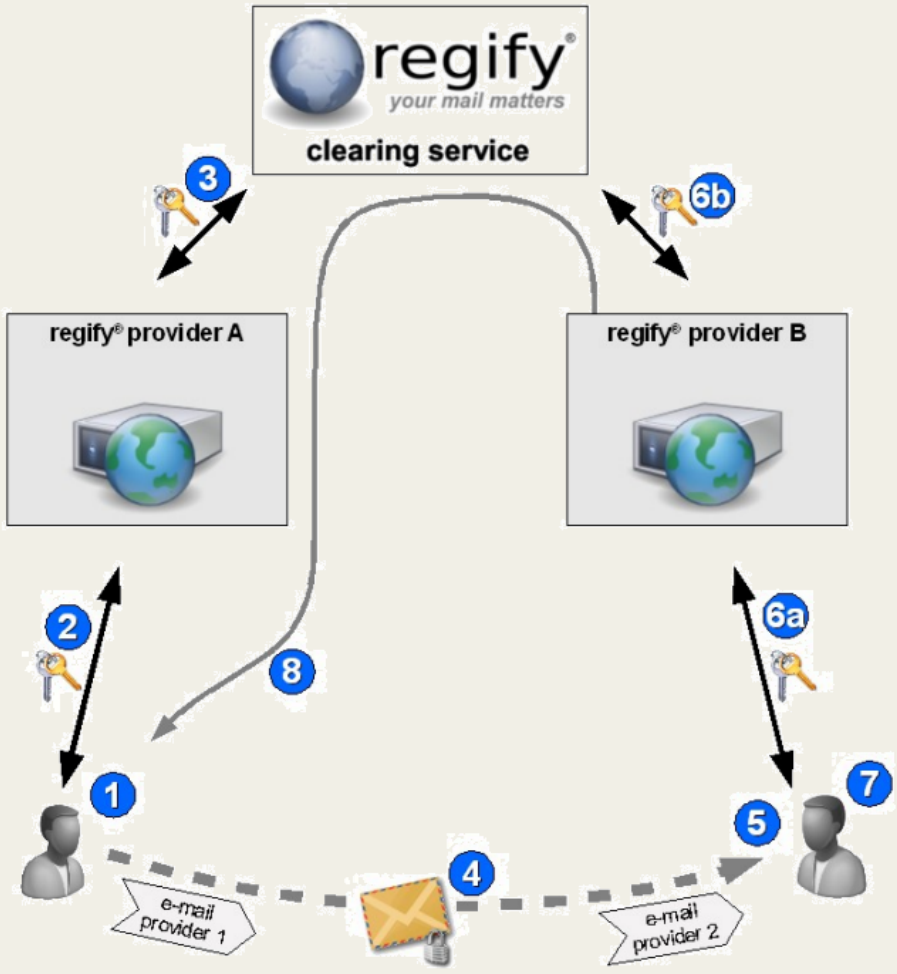
Règles du moteur d'habilitation

- Consentement
- Mandat
- Profil
- Liste noire (Blacklist)
- Liste blanche (Whitelist)
- Niveau d'accès
- Niveau de confiden-tialité du document

SSO - Contrôle Applicatif des Accès



Cryptage des échanges



Merci

ebrc
TRUSTED DATACENTRE, CLOUD & MANAGED SERVICES

AGENCE eSanté LUXEMBOURG