SECURITE SOUS WINDOWS VISTA.

PROBLEMATIQUE ET IMPACT SUR LE DEVELOPPEMENT D'APPLICATIONS.

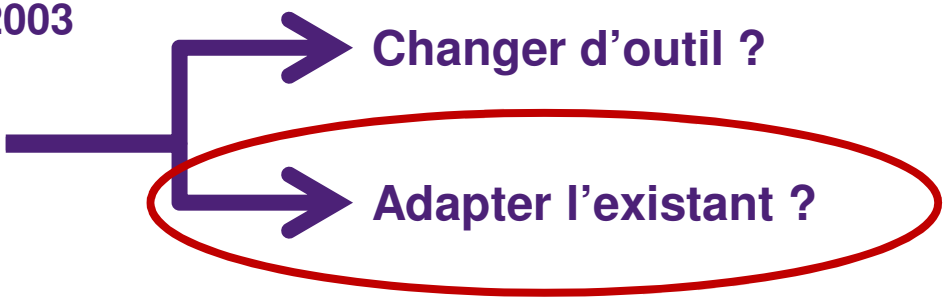
9 janvier 2009

Emmanuel.Chiarello@sig-ge.ch

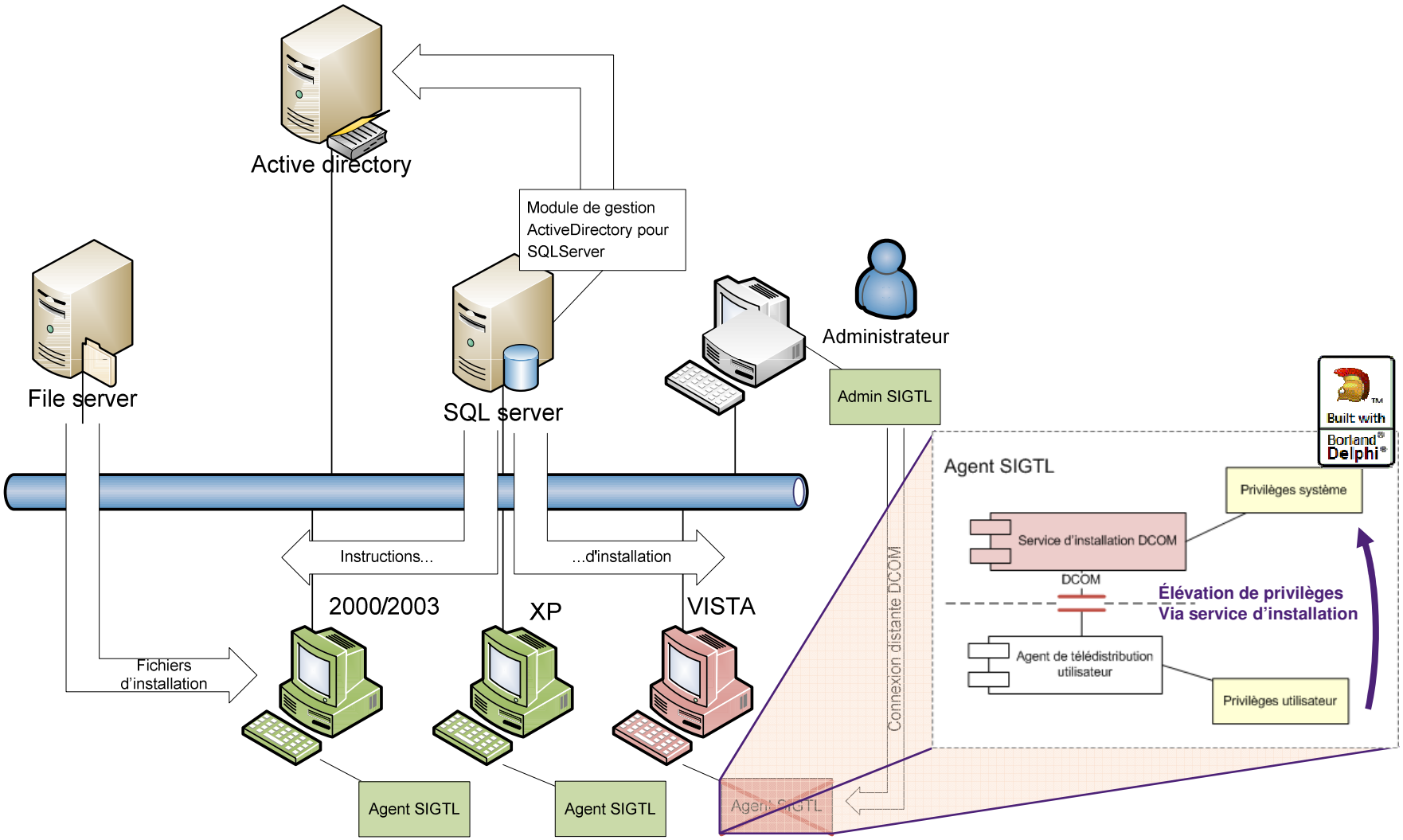
Contexte: programme de télédistribution SIGTL sous Windows VISTA

- **Télédistribution ?**
  - ► Automatiser l'installation des logiciels
  - ► Plus d'interventions manuelles (baisse des coûts)
  - ► Installations reproductibles (gain de qualité)

- **Programme développé à SIG et utilisé depuis 1997**
  - ☺ Windows 3.11 & NT4 (16/32 bits)
  - ☺ Windows 2000
  - ☺ Windows XP & 2003
  - ☹ Windows VISTA



Principe de fonctionnement général



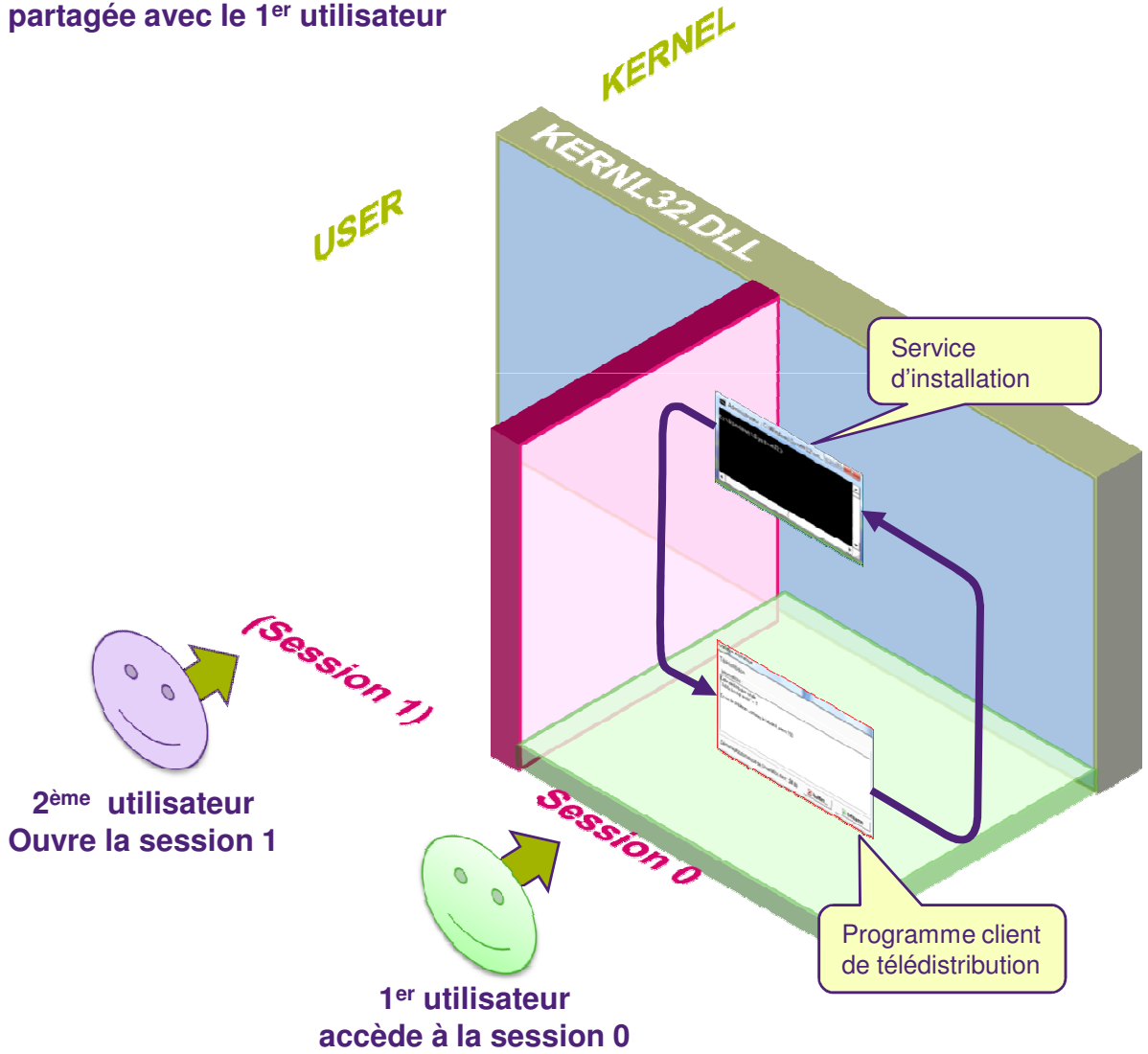
Analyse des mécanismes de sécurité Windows Vista

Spécification du système	Analyse	Conception
Intégration	Validation	Implémentation

- **Maîtrise:**
  - Des principes de sécurité des objets Windows
  - Des nouveaux mécanismes de sécurité de Windows Vista:
    - **MIC**, le contrôle d'intégrité obligatoire
    - **UIPI**, le contrôle d'intégrité pour les objets USER
    - **UAC**, le contrôle de compte utilisateur
      Consentement utilisateur pour lancer un processus administrateur
      - **Objectif: Contrôler l'escalade de privilège**
        Problème de sécurité N°1 sous XP
- **Développement de l'outil SecurityExplorer**
  - Visualiser les attributs de sécurité des objets Windows
  - Un + pour le développement sous Windows !

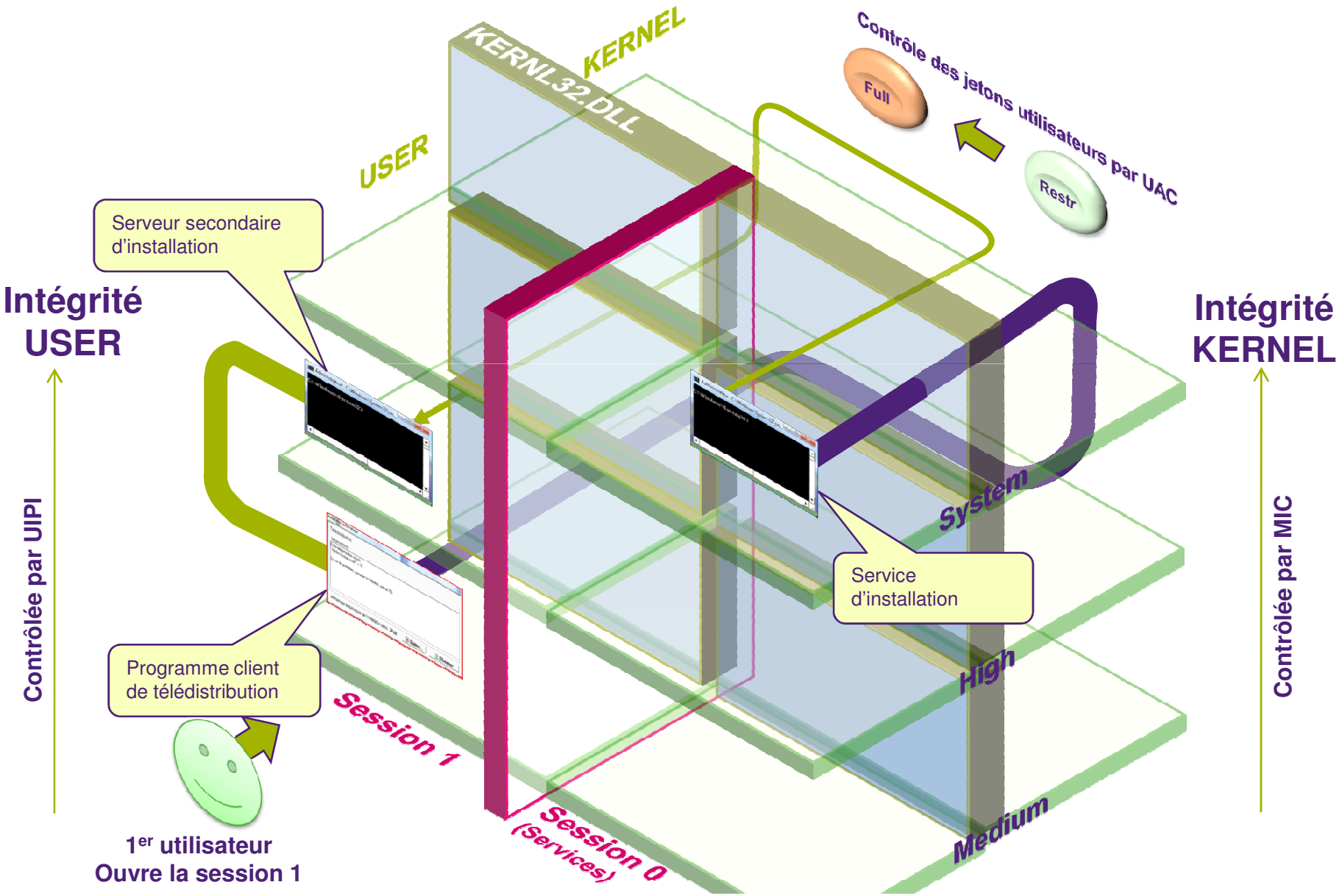
Isolation des processus sous XP

Session 0
- **session des services**
- **partagée avec le 1er utilisateur**



Isolation des processus sous VISTA

Spécification du système	Analyse	Conception
Intégration	Validation	Implémentation



Mécanisme RPC ad-hoc par named-pipe

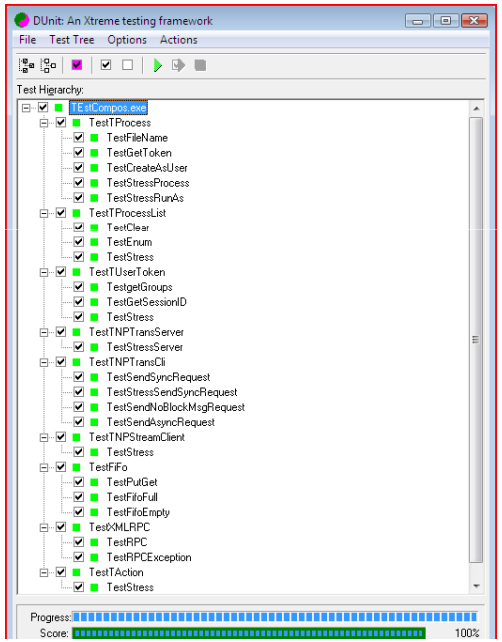
Spécification du système	Analyse	Conception
Intégration	Validation	Implémentation

- ☹ Trop de barrières à franchir pour continuer à utiliser COM/DCOM
  - ► Sessions
  - ► Niveaux d'intégrité contrôlés par MIC et UIPI
- ☹ Framework RPC Windows difficilement accessible sous Delphi
  (contrainte de l'existant)

- ☺ Named-pipe = bon candidat
  - ► Contrôle d'accès
  - ► Authentification du client
  - ► Accessible à distance
  - ☑ Appels RPC sérialisés en XML
  - ☑ Gestion multithreads des IO

Tests unitaires

- Batterie de tests permettant la validation des principales méthodes des classes développées.
- Contrôle des fuites mémoire par extension du framework de tests Delphi



Analyse de risque I
Mesure de qualité

- **Evaluation de la « qualité » (solidité / confiance) du code par le calcul des métriques**
  - **Complexité cyclomatique (Notion introduite en 1976 par Thomas McCabe)**
    - **Mesure le nombre de chemins indépendants dans le code source**

$$1 + \sum Branches + \sum Boucles + \left(\sum ET\ logiques + \sum OU\ logiques\right)_{expressions\ \ conditionnelles}$$

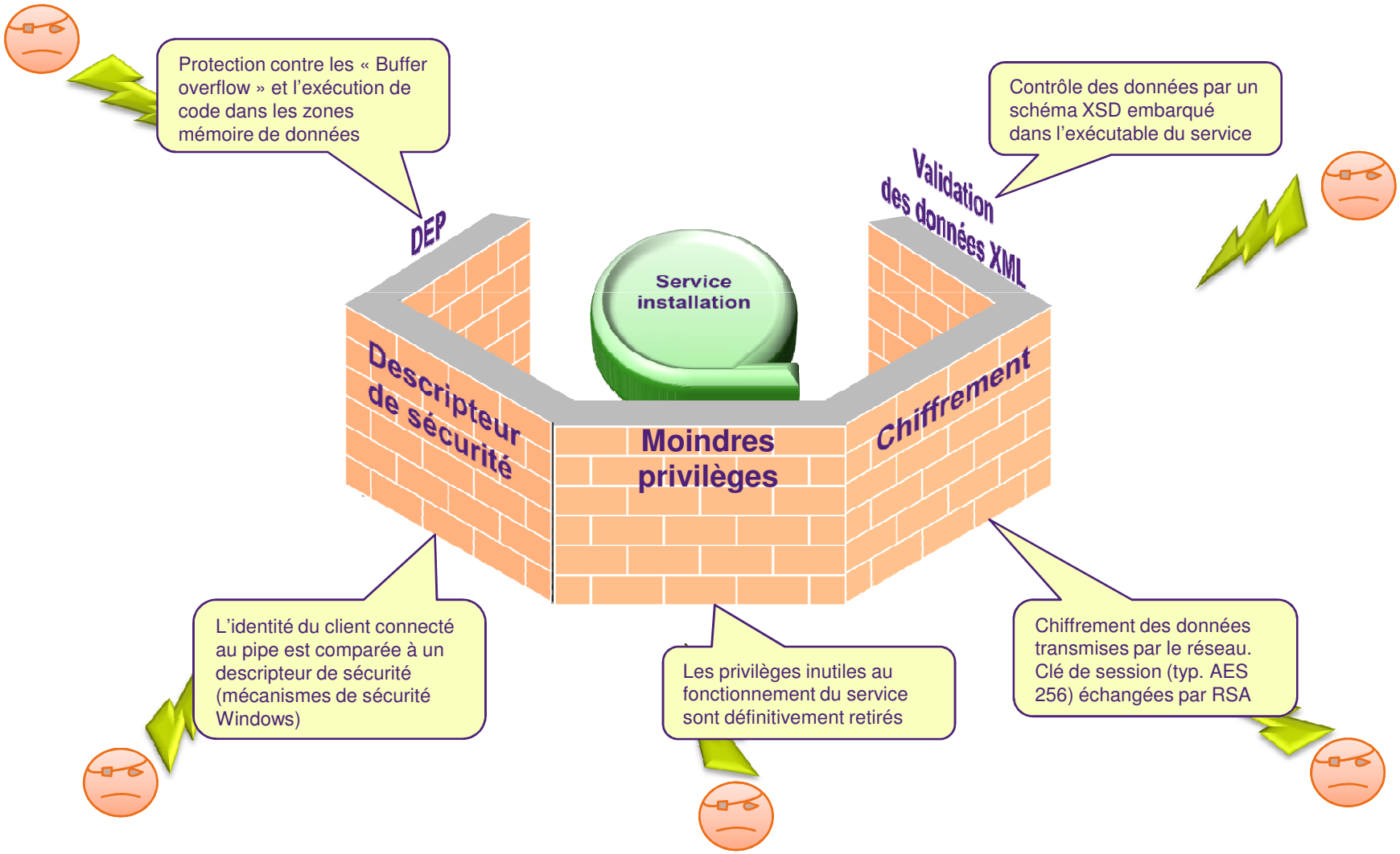
    - **Grande complexité cyclomatique = risque élevé:**
      - 1-10 Simple, risque faible
      - 11-20 Plus complexe, risque modéré
      - 21-50 Complexe, risque élevé
      - + 50 Instable, risque très élevé

CodeHealer for Delphi

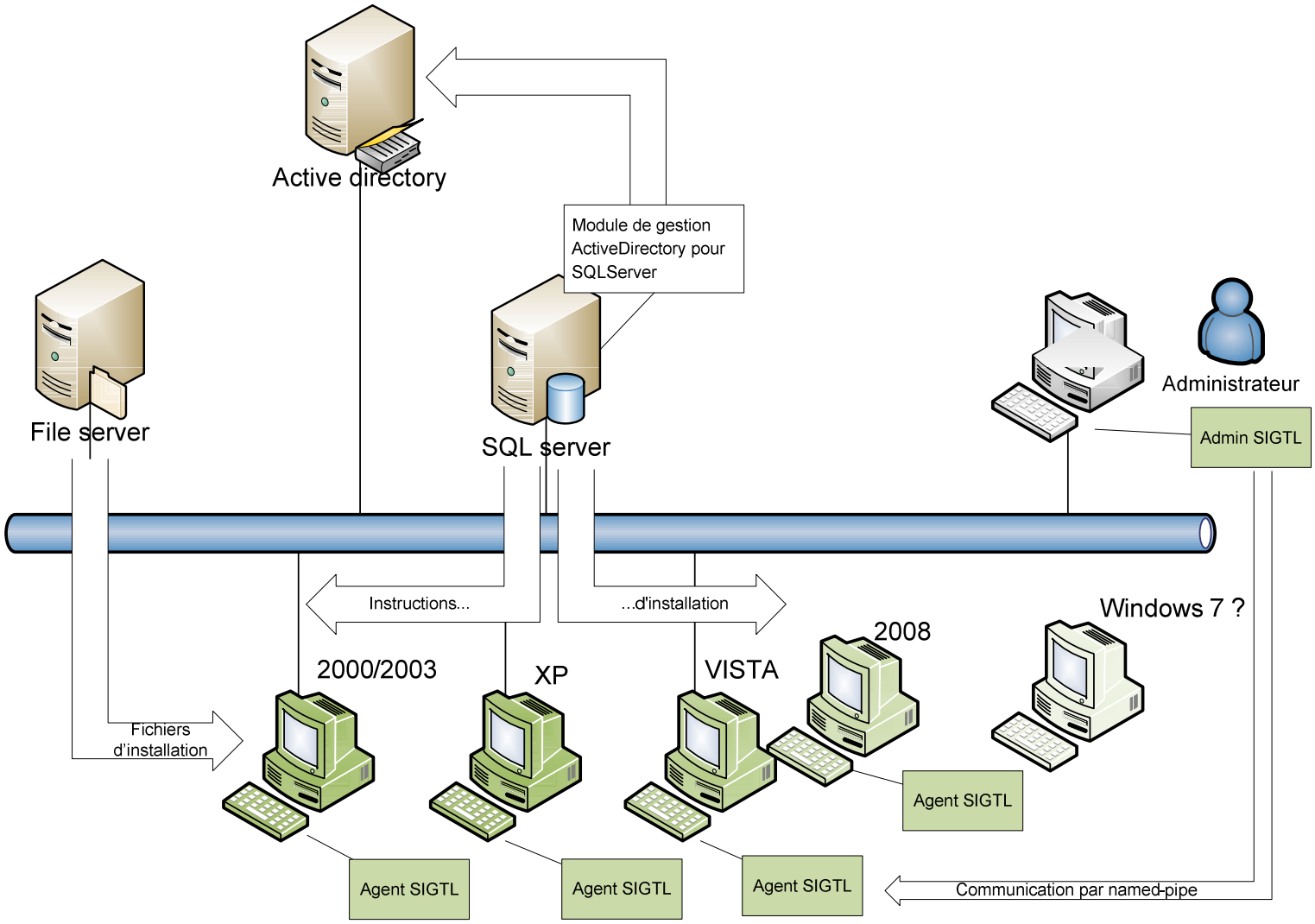
SOCK
Specialists Of Computer Knowledge
SOFTWARE

    - **L'unité la plus complexe du projet est à 6, moyenne = 4 ☺**

Analyse de risque II
« Hardening » du service d'installation



Pour finir…


Active directory
Module de gestion ActiveDirectory pour SQLServer
File server
SQL server
Administrateur
Admin SIGTL
Instructions...
...d'installation
2000/2003
XP
VISTA
2008
Windows 7 ?
Fichiers d'installation
Agent SIGTL
Agent SIGTL
Agent SIGTL
Agent SIGTL
Communication par named-pipe

Démo

Spécification du système	Analyse	Conception
Intégration	Validation	Implémentation