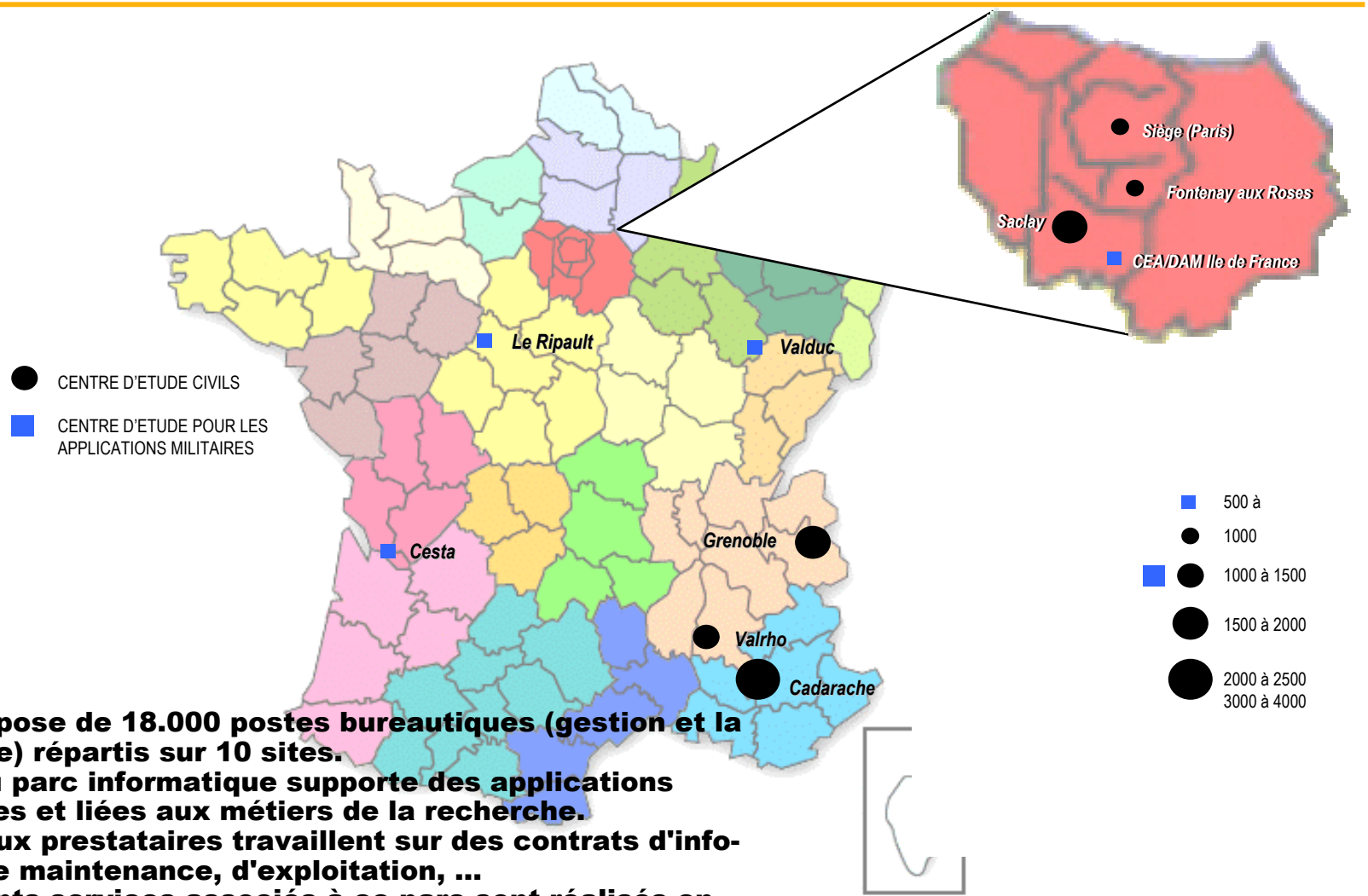
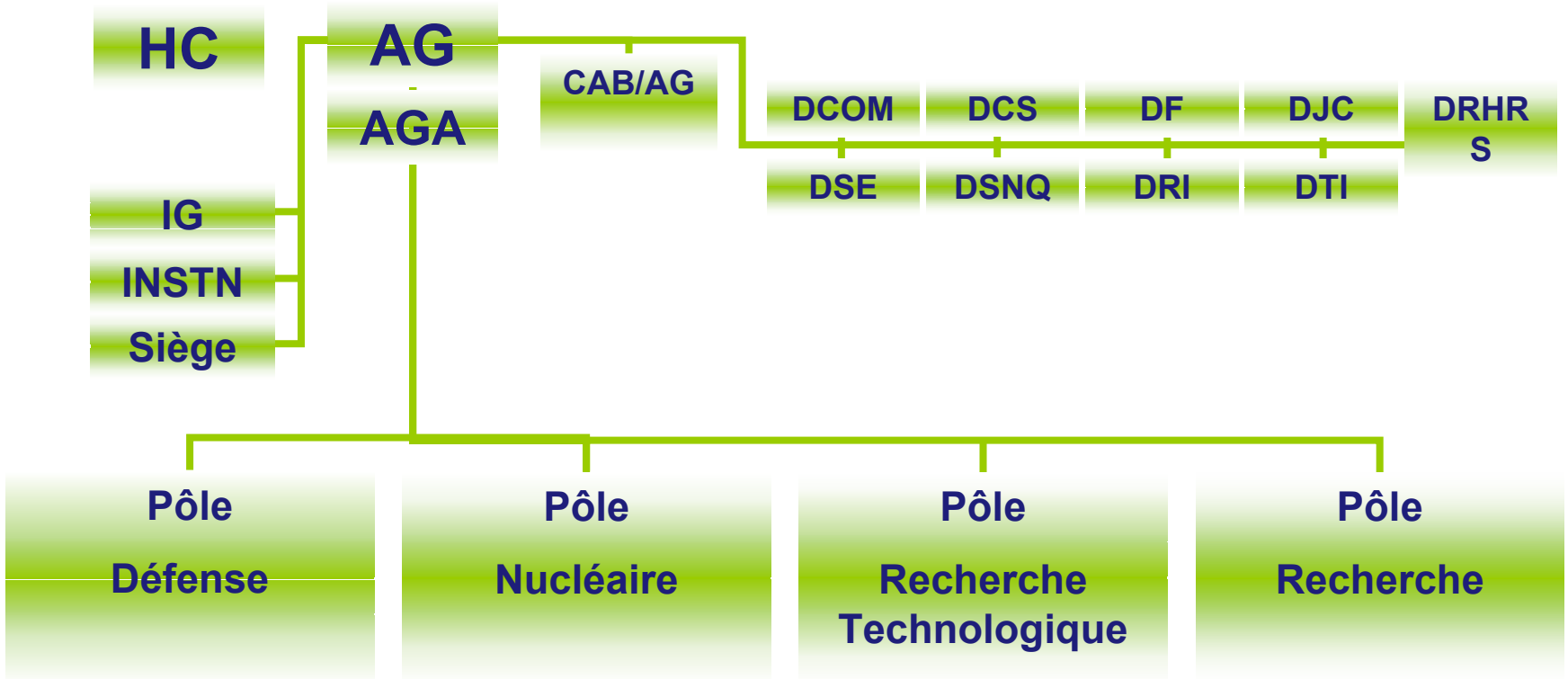
Déploiement d'application de traitement d'informations sensibles dans les centres civils du CEA

Informatique au CEA



Le CEA dispose de 18.000 postes bureautiques (gestion et la bureautique) répartis sur 10 sites.
Le reste du parc informatique supporte des applications scientifiques et liées aux métiers de la recherche.
De nombreux prestataires travaillent sur des contrats d'info-gérance, de maintenance, d'exploitation, ...
Les différents services associés à ce parc sont réalisés en interne ou sous-traités

Organisation du CEA



Contexte du CEA (1/2)

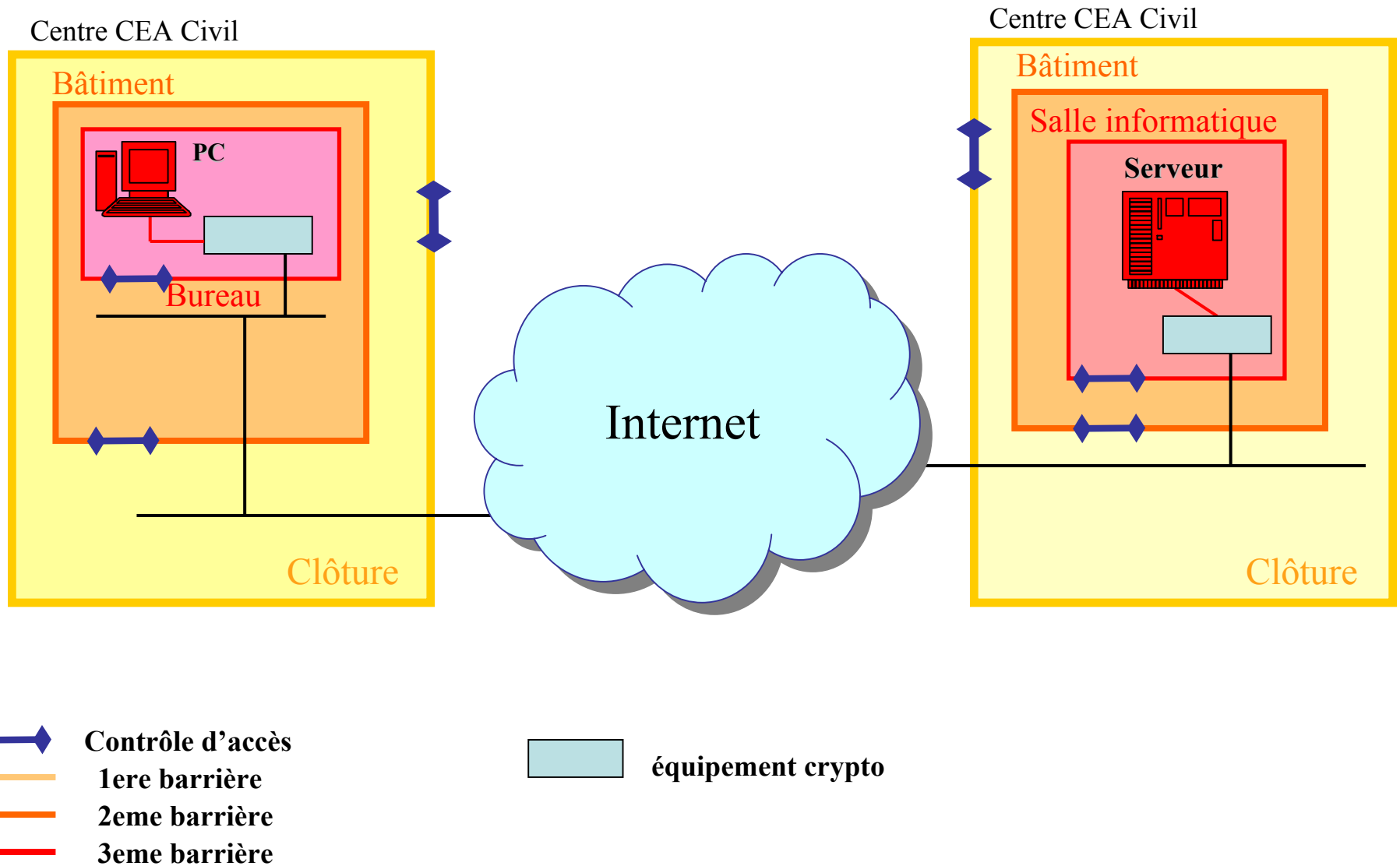
- Objectifs SSI des applicatifs sensibles
  - C (3), I (3), D (1)
  - imputabilité des actions
- Menaces
  - principalement internes :
    - utilisateurs des applicatifs
    - autres collaborateurs

Contexte du CEA (2/2)

Contrainte de développement

- Prise en compte de la réglementation interne
  - protection physique des informations traitées
  - catalogue des produits
- Prise en compte de l'existant CEA
  - architecture client/serveur
  - référentiel de développement,
    - actuellement client Citrix (référentiel CEA/Normacs)
      à terme navigateur (référentiel J2EE)
  - serveurs (pour mémoire)
  - liaison par le réseau CEAnet

Zones de protection physique



Solution « classique »

- Protection physique des locaux
  - Coût ~ 5000€ par bureau isolé
  - Chiffrement en « coupure » pour la protection des informations en transit
    - Coût (investissement) :
      - ~ 8500€ par poste de travail (et/ou installation)
      - ~ 85000€ centre de gestion de clefs
    - Coût (fonctionnement - personnel) :
      - ~ 4 personnes /centre/temps partiel
      - ~ 4 personnes/national/mi-temps
- Inconvénients :
  - Peu de produits disponibles
  - Coût

Solution proposée

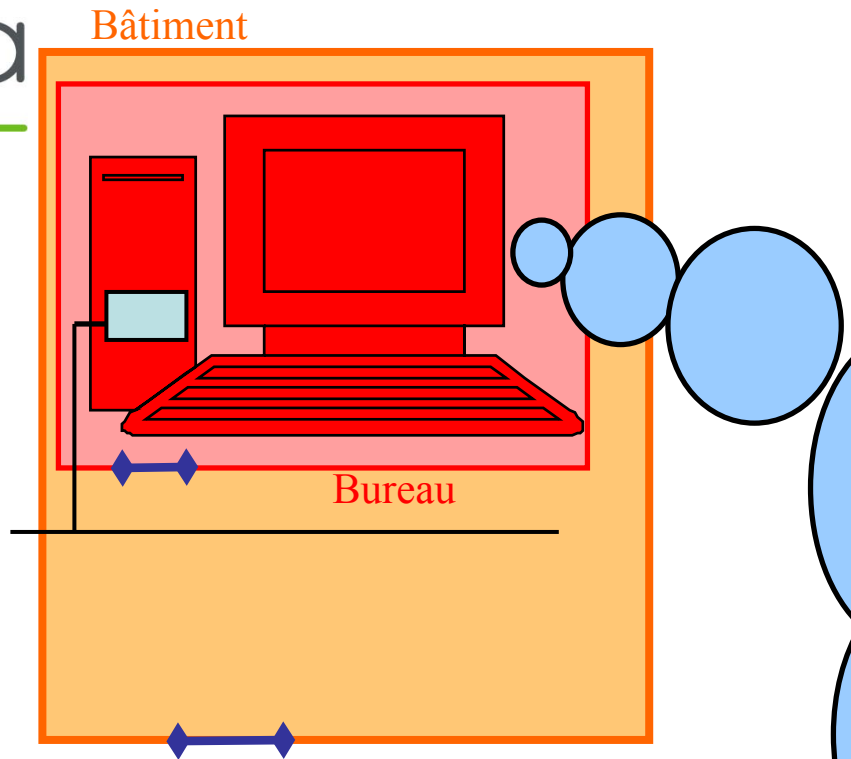
- Protection physique des locaux
  - Coût ~ 5000€ par bureau isolé
- Poste de travail léger
  - base PC standard
  - logiciels sur base Open Source (Linux, …)
  - architecture VPN
- Coûts
  - postes de travail « standard », pas de licences
  - exploitation réduite
  - agrément ???

Protection physique / Protection logique

- Protection physique avec pour objectifs :
  - Détection de l'intrusion
  - Retardement de l'intrusion

- Protection logique :
  - Possession de dispositifs physiques
    - Carte(s) à puce (admin, utilisateur)
    - CD chiffré de l'application
  - Connaissance d'un élément (pin code)
  - Poste de travail protégé
    - Logiciel du poste protégé par chiffrement
    - Démarrage du poste de travail contrôlé
  - Authentification des accès au réseau (VPN)
  - Authentification des accès à l'application
  - « Logs » possible à plusieurs niveaux

Résumé des spécifications

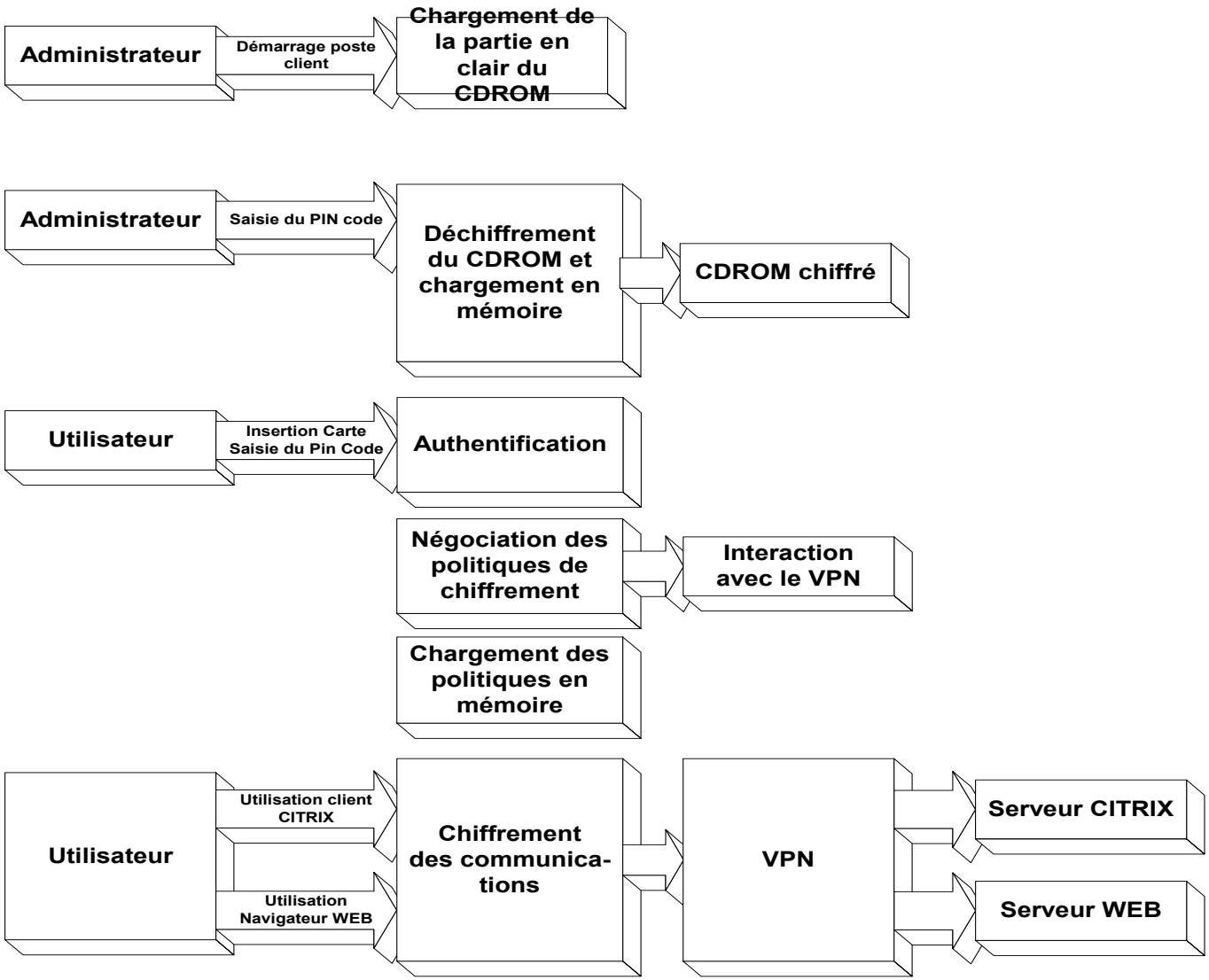


Module logiciel crypto

Poste de travail sécurisé :

- système d'exploitation maîtrisé
- pas de stockage rémanent
  - pas de disque
  - pas de disquette
  - …
- Authentification forte
  - carte à puce
- Logiciel non modifiable
  - inscrit en ROM ou sur CD-Rom

Authentification au démarrage du PC



QUESTIONS

laurent.cabirol@cea.fr