ASPIC - Cert@too

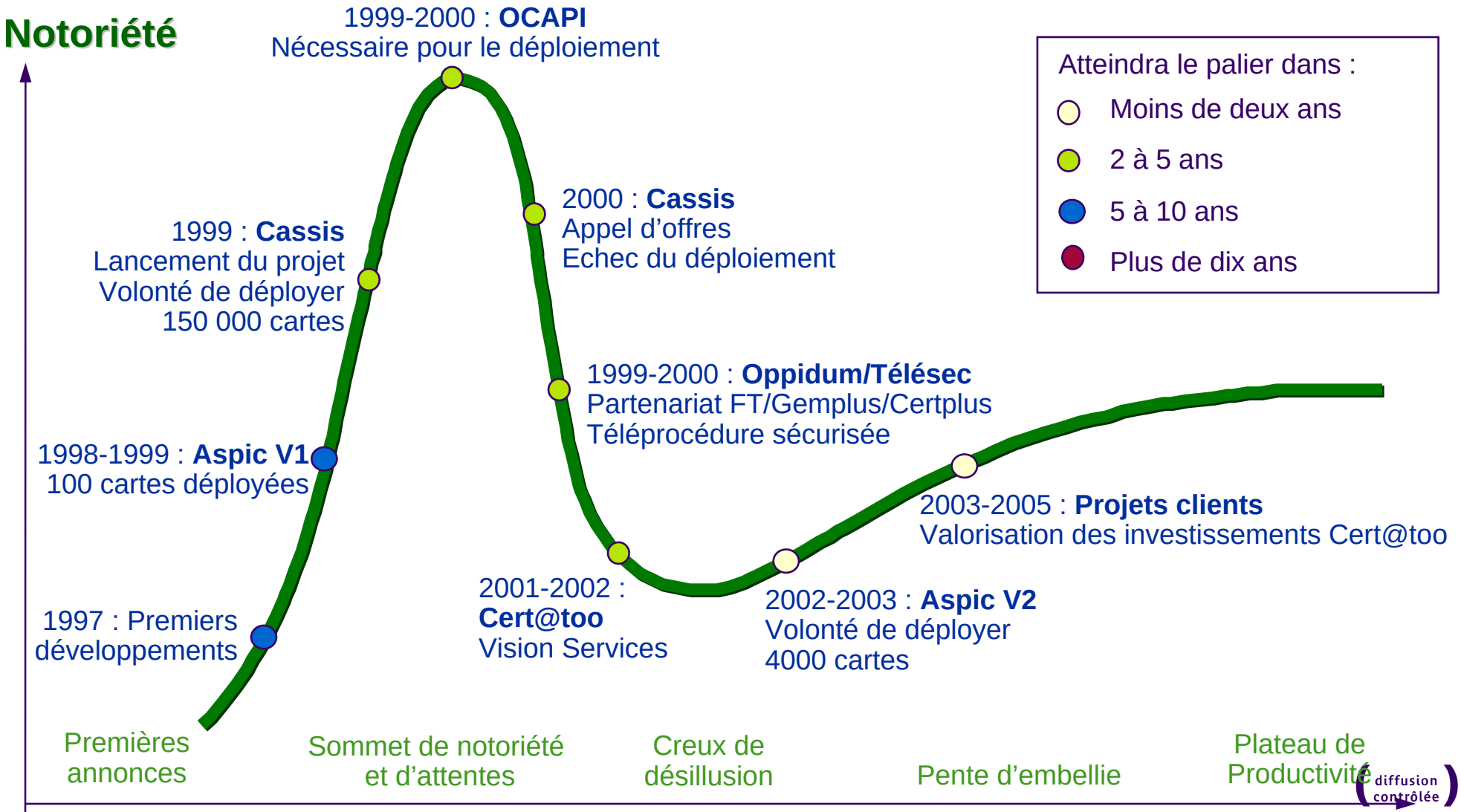
JSSI 2003

Dimitri MOUTON (FTR&D/DTL/SSR)

dimitri.mouton@rd.francetelecom.com

Cert@too : Emergence de la PKI

The Gartner 2002 Hype Cycle of Emerging Technologies



Cert@too : Les objectifs du projet

- **Développer l'offre de services sécurisés**
- **Fournir une architecture de sécurité commune à ces services**
- **Mieux connaître l'offre du marché des supports cryptographiques**
- **Réduire les coûts de la PKI et maîtriser sa configuration**

Cert@too : Les quatre chantiers

SERV@TOO — ***Les services sécurisés***

- Téléprocédures
- Publication de documents signés
- Chiffrement de données
- Signature de groupe
- Workflow sécurisé

APPL@TOO — ***La plate-forme de sécurité***

- Signature électronique
- Chiffrement / déchiffrement
- Horodatage
- Confiance
- Protocole SSL

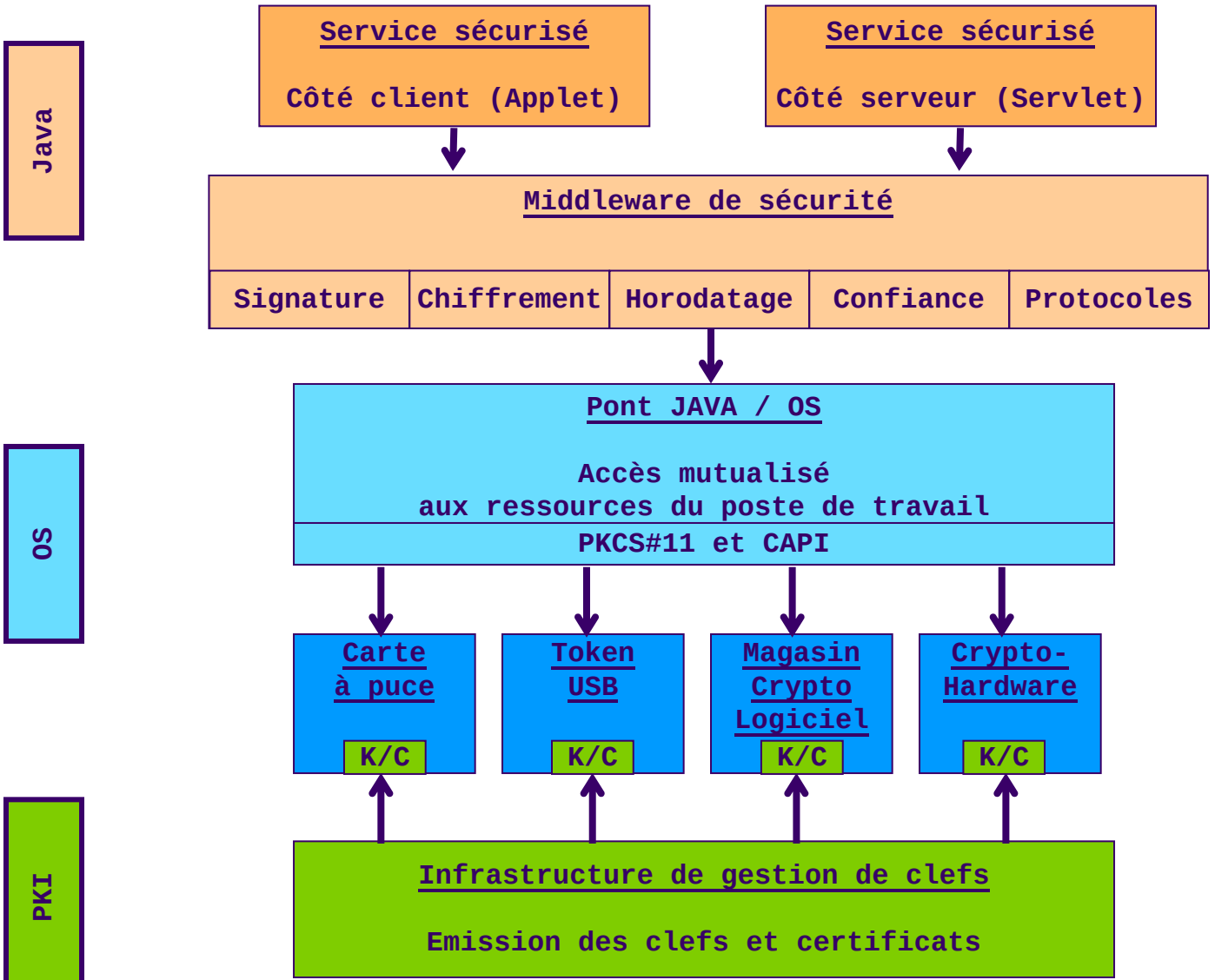
CART@POO — ***Les supports cryptographiques***

- Cartes à puce
- Dongles USB
- Magasins logiciels
- Crypto-hardwares

IC@POO — ***L'infrastructure à clefs publiques***

- Emission et gestion des certificats
- Emission et gestion des clefs
- Adaptation aux besoins des clients
- Configuration des traitements
- Ouverture aux évolutions
- Conformité aux standards

Cert@too : L'architecture



➔ *Serv@too*

➔ *Appl@too*

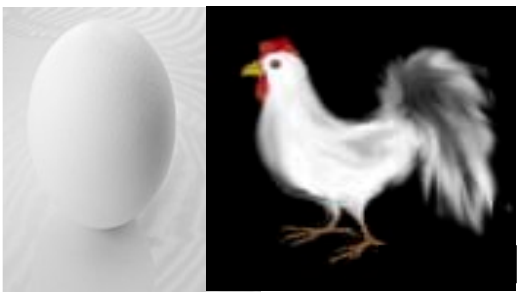
➔ *Cart@poo*

➔ *Ic@poo*

diffusion contrôlée

Infrastructure – services...

Un problème d'œuf et de poule !



- ✓ **Pas de service sans infrastructure**
- ✓ **Pas de rentabilité de l'infrastructure sans service**

ASPIC : la PKI FTR&D

ou comment sortir de cette problématique

Aspic – les PKI – Cert@too...

- **VPN – IPSEC (Windows et Linux) sur :**
  - **802.11**
  - **ADSL (PPPOE- PPPOA)**
  - RTC Wanadoo
  - LAN
  - Bluetooth
  - Inmarsat
  - RTC NAS
  - GSM wanadoo/NAS
  - GPRS wanadoo/NAS

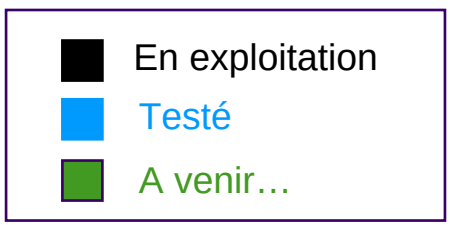
CERT@TOO

- **Services de confiance**
  - **Messagerie chiffrée signée**
  - Accès serveur WEB sécurisé (SSL)
  - **Workflow sécurisé (Orange)**
  - Téléprocédures
  - **Dématérialisation de flux papier**
  - Publication/consultation de documents chiffrés et/ou signés, horodatés
  - Signature de groupe

MaiLegal

- Lettre recommandé avec AR

- **Applications sur le poste de travail**
  - **Login Windows**
  - Chiffrement du disque dur
  - SSO
  - …



Questions - Réponses

➔MERCI !

➔A vous...

Matériel - logiciel

- VPN – cisco
  - Gateway : VPN concentrateur 3030
  - Client : client cisco (V3.6.1 septembre 2002)
- Carte à puce e-gate cryptoflex 32 k (Schlumberger)
- Lecteur de carte à puce
  - USB
  - porte clé ou lecteur

VPN - IPSEC

Tunnel IPSEC :
- **Authentification mutuelle des extrémités**
- **Confidentialité**
- **Intégrité**

Poste client

Réseau d'entreprise

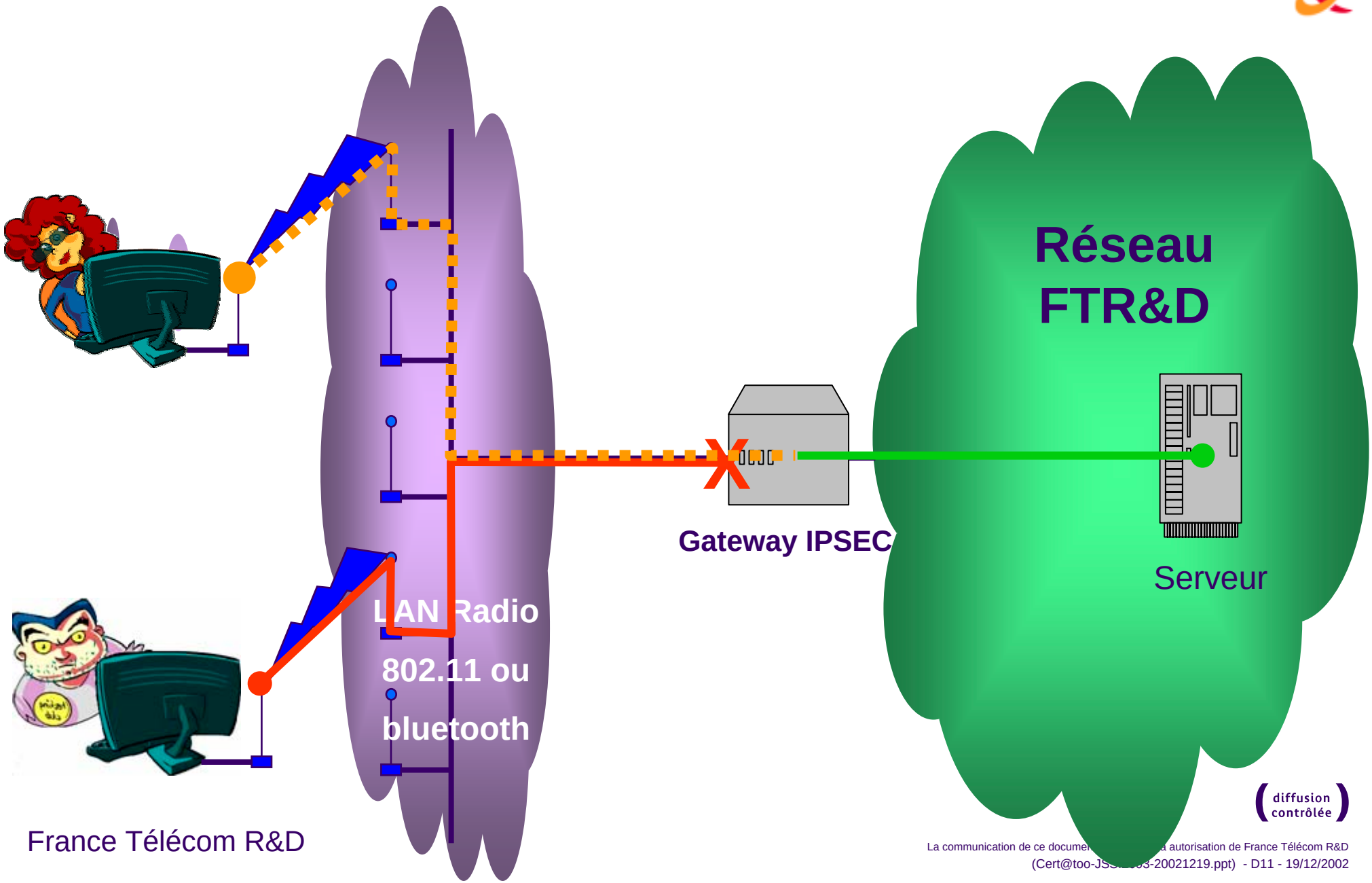
Gateway IPSEC

Serveur

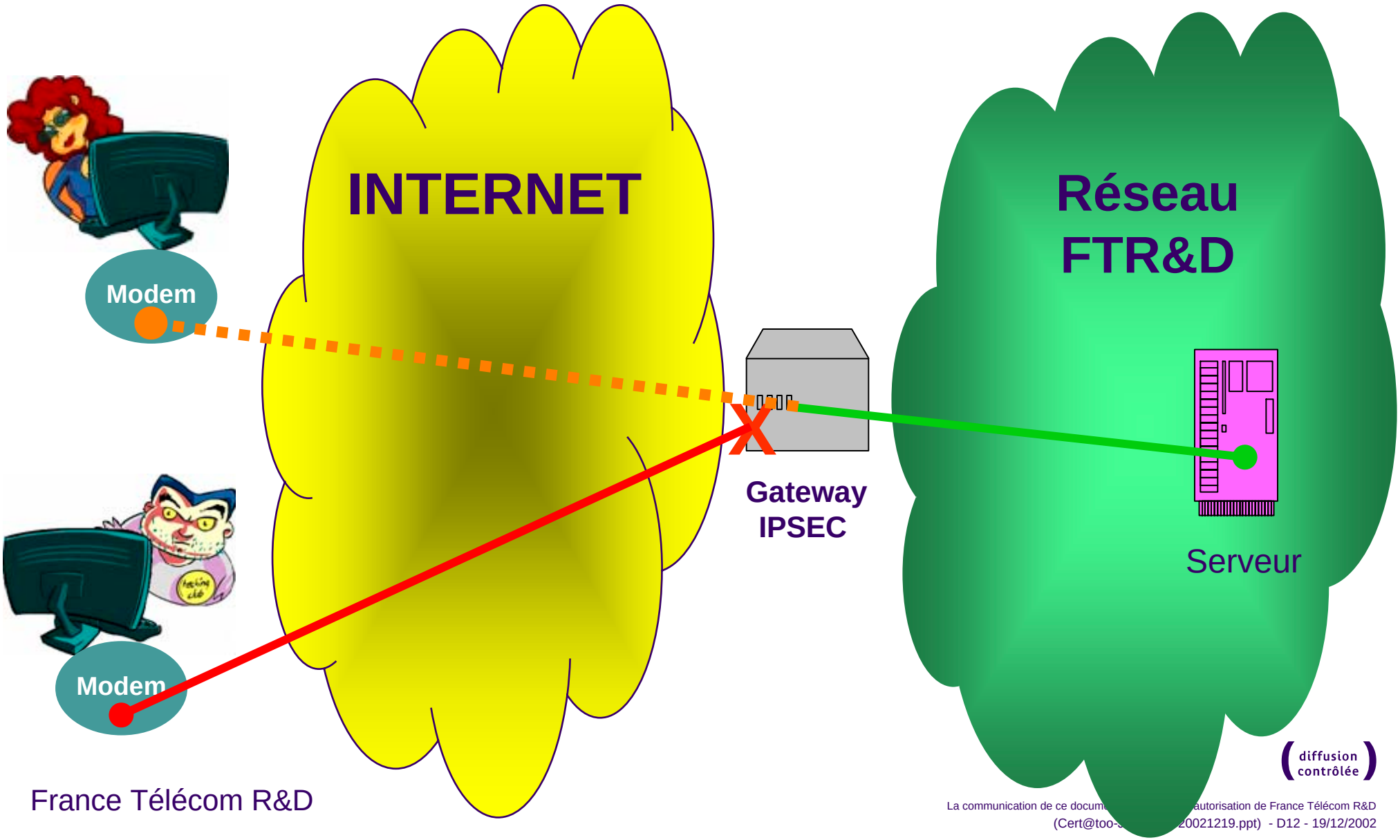
Plusieurs réseaux (de type différents)

diffusion contrôlée

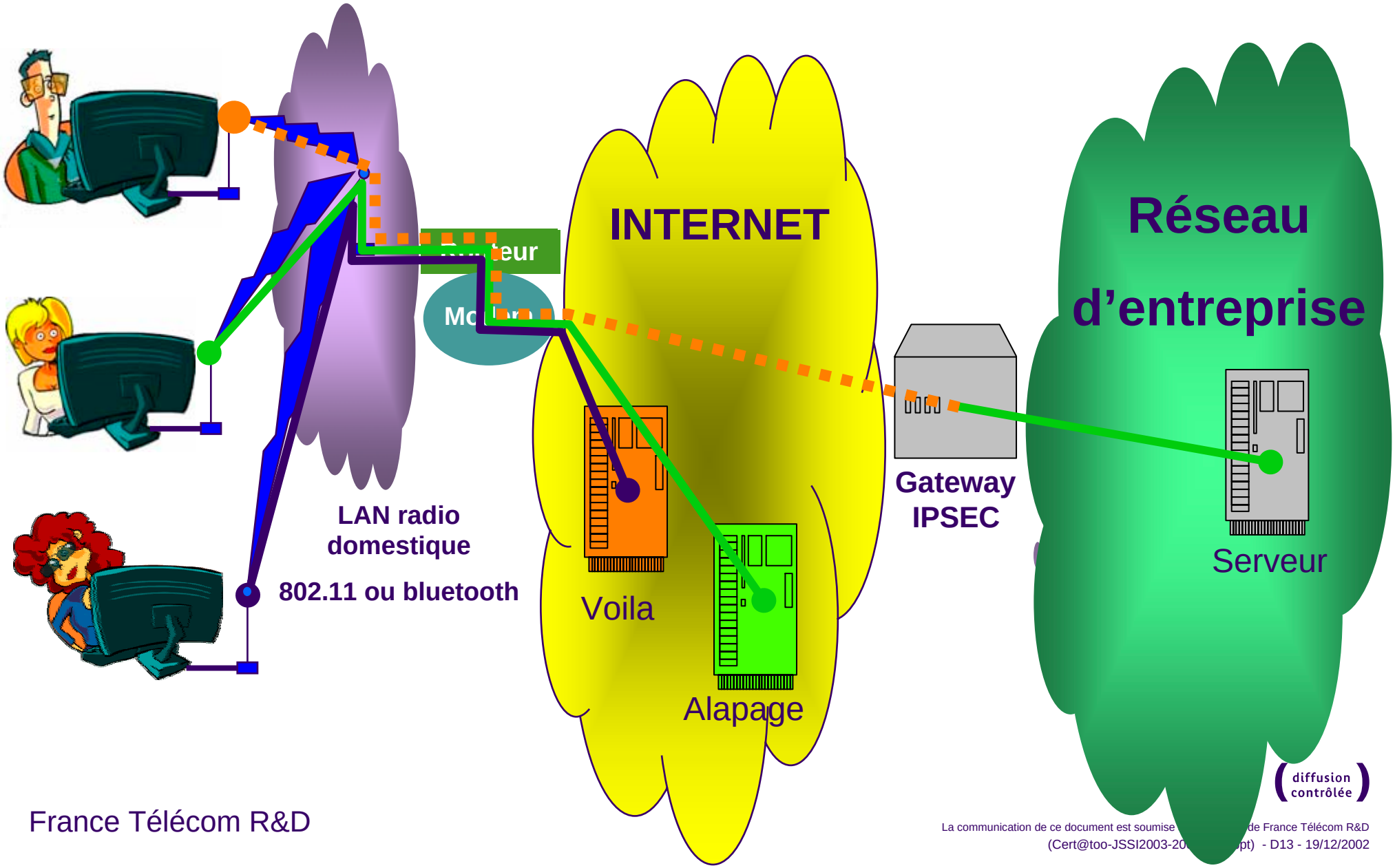
VPN – IPSEC sur 802.11 ou bluetooth



VPN – IPSEC sur ADSL



VPN IPSEC sur ADSL + LAN radio domestique



France Télécom R&D