



# ASPIC - Cert@too

## JSSI 2003

**Dimitri MOUTON (FTR&D/DTL/SSR)**

dimitri.mouton@rd.francetelecom.com

Le présent document contient des informations qui sont la propriété de France Télécom. L'acceptation de ce document par son destinataire implique, de la part de ce dernier, la reconnaissance du caractère confidentiel de son contenu et l'engagement de n'en faire aucune reproduction, aucune transmission à des tiers, aucune divulgation et aucune utilisation commerciale sans l'accord préalable écrit de France Télécom R&D

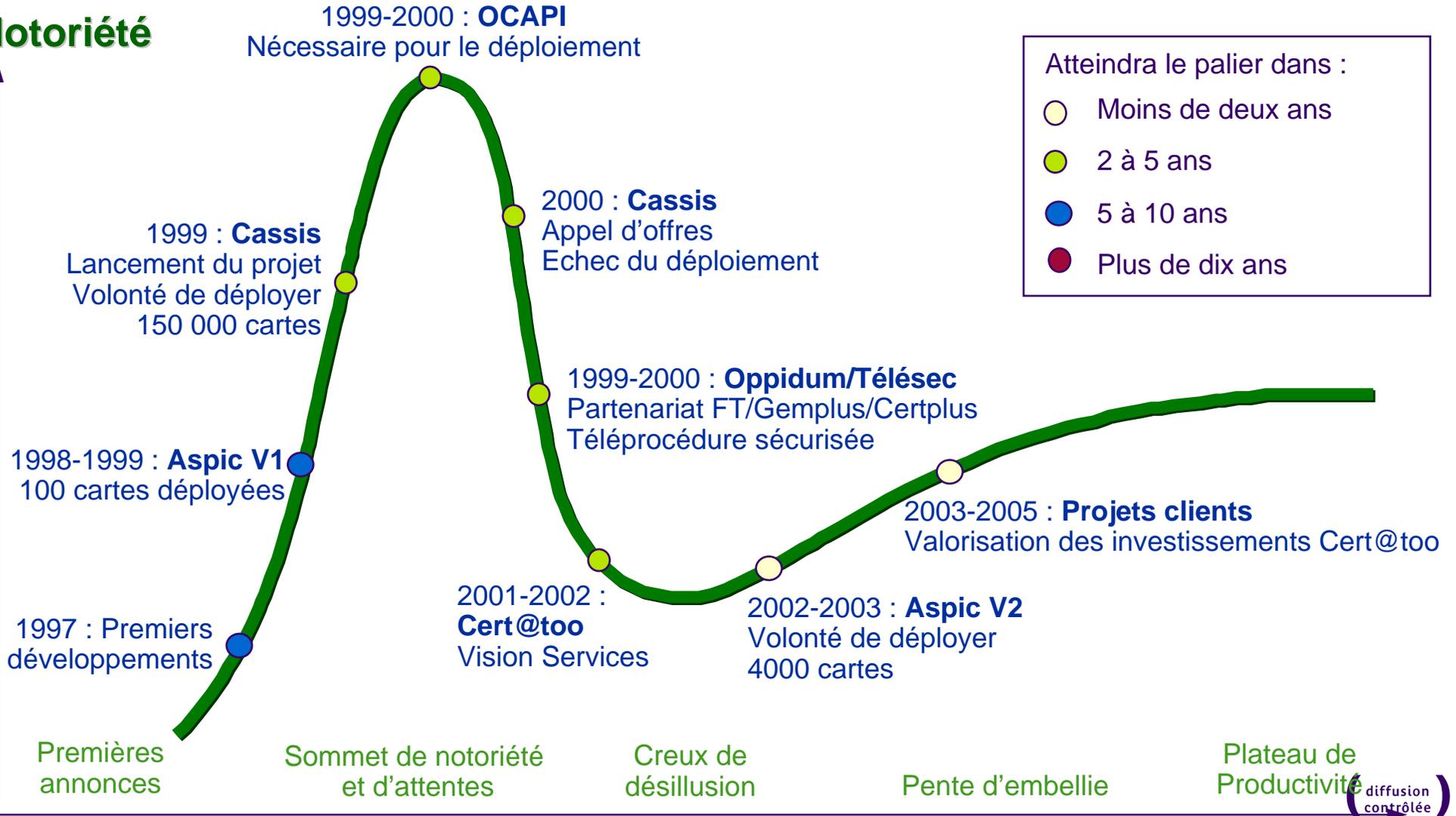
( diffusion  
contrôlée )

# Cert@too : Emergence de la PKI



## The Gartner 2002 Hype Cycle of Emerging Technologies

### Notoriété



# 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

(diffusion  
contrôlée)

# Cert@too : L'architecture



Java

Service sécurisé  
Côté client (Applet)

Service sécurisé  
Côté serveur (Servlet)

→ **Serv@too**

Middleware de sécurité

Signature	Chiffrement	Horodatage	Confiance	Protocoles
-----------	-------------	------------	-----------	------------

→ **Appl@too**

OS

Pont JAVA / OS

Accès mutualisé  
aux ressources du poste de travail

PKCS#11 et CAPI

Carte à puce

K/C

Token USB

K/C

Magasin Crypto Logiciel

K/C

Crypto-Hardware

K/C

→ **Cart@poo**

PKI

Infrastructure de gestion de clefs

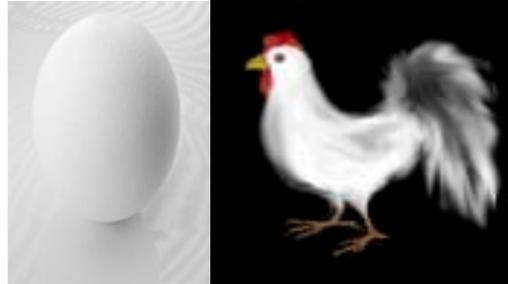
Emission des clefs et certificats

→ **Ic@poo**

# 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

C  
E  
R  
T  
@  
T  
O  
O

MaiLegal

## → 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
  
- ▶ Lettre recommandé avec AR

## → Applications sur le poste de travail

- ▶ Login Windows
- ▶ Chiffrement du disque dur
- ▶ SSO
- ▶ ...

■	En exploitation
■	Testé
■	A venir...

(diffusion  
contrôlée)

# 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

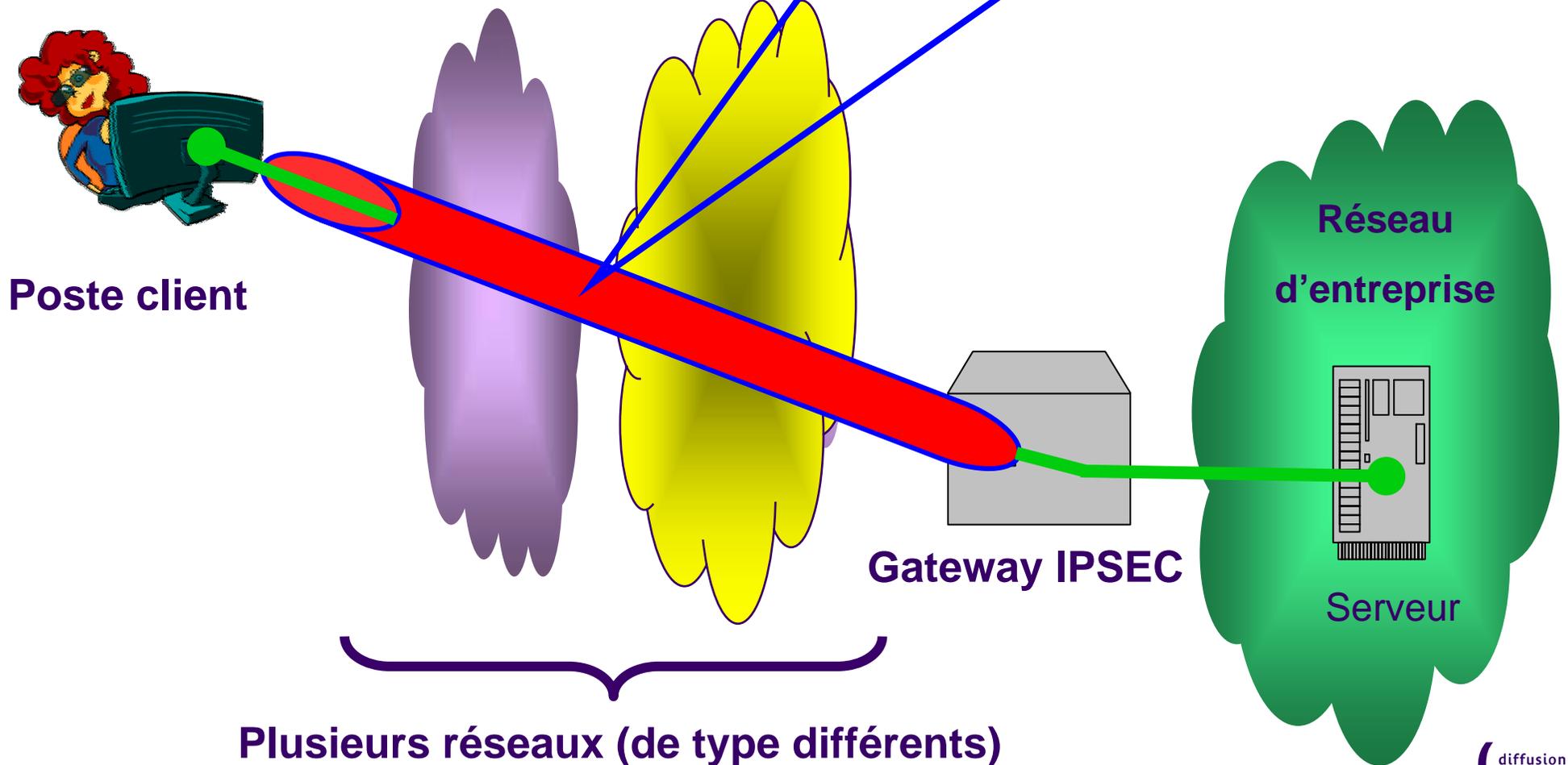
- ▶ USB
- ▶ porte clé ou lecteur

# VPN - IPSEC



## Tunnel IPSEC :

- Authentification mutuelle des extrémités
- Confidentialité
- Intégrité



Poste client

Réseau  
d'entreprise

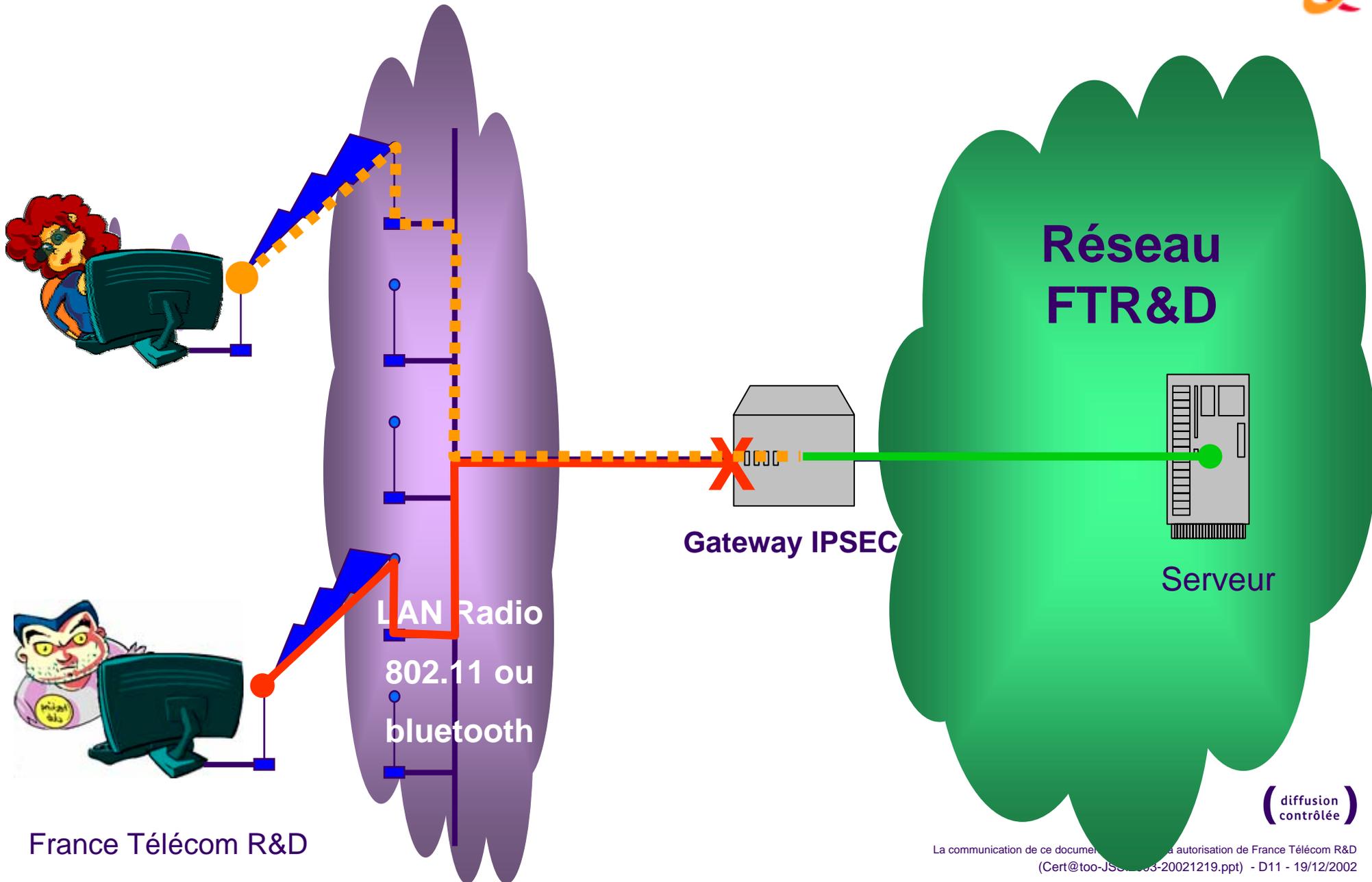
Gateway IPSEC

Serveur

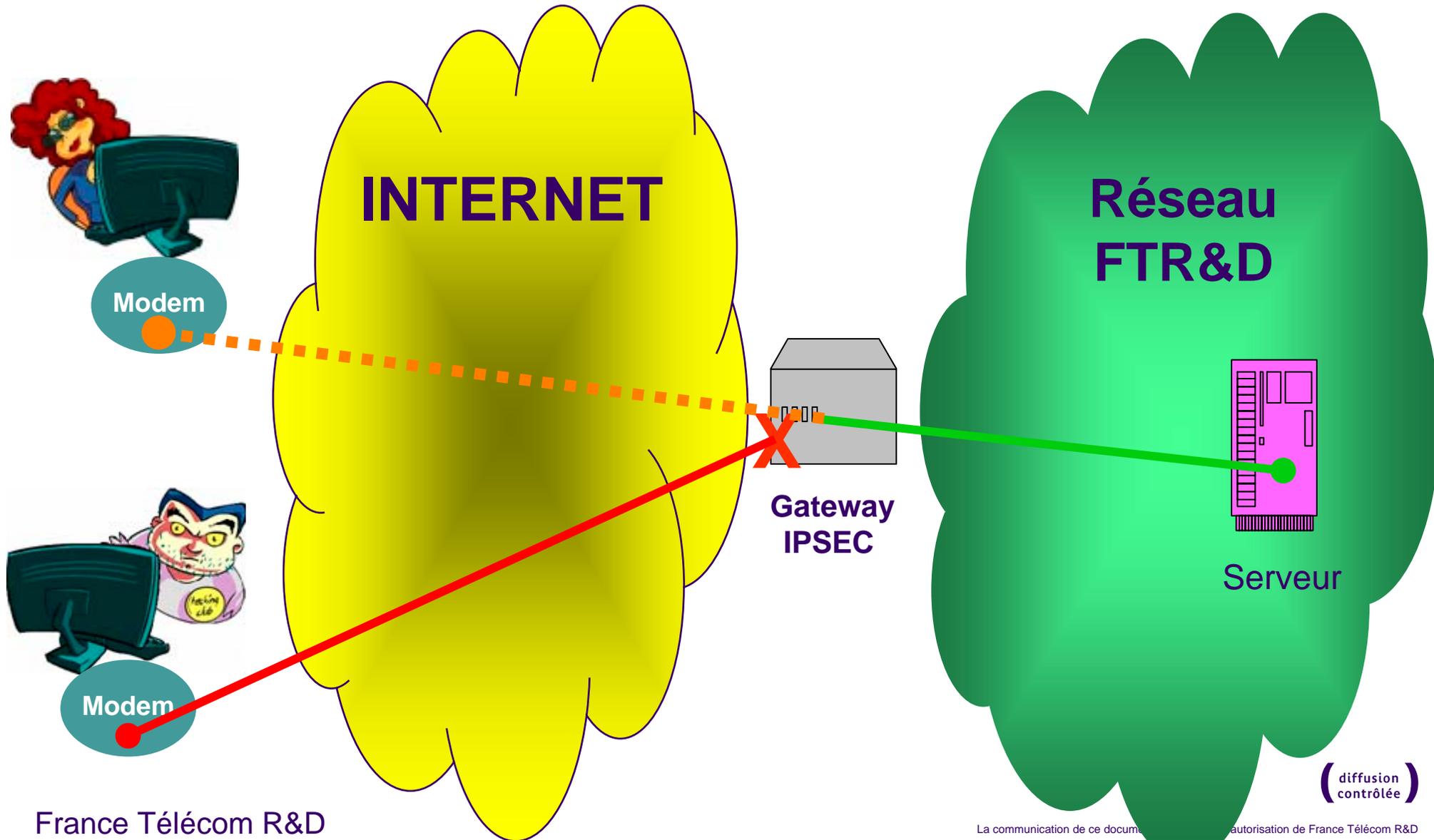
Plusieurs réseaux (de type différents)

(diffusion  
contrôlée)

# VPN – IPSEC sur 802.11 ou bluetooth



# VPN - IPSEC sur ADSL



# VPN IPSEC sur ADSL + LAN radio domestique

