

Jeudi 12 juin 2008
de 14h00 à 15h00



Sécurité des réseaux et solutions

État des lieux des solutions existantes et à venir

Benjamin CHARLES
Bluesafe

Damien SAUVERON
XLIM (UMR Université de
Limoges/CNRS 6172)



wistp'07

Workshop in Information
Security Theory and Practices

May 8-11, 2007

1st edition HERAKLION, Greece



**“ Smart Cards,
Mobile and Ubiquitous
Computing Systems ”**

► **May 11, 2007**
dedicated day to:

**Networking meeting to discuss
proposals for the EU FP7**

For further information: <http://wistp2007.xlim.fr/>
If you are interested, please contact us at: wistp2007@xlim.fr



GLOBALPLATFORM



INSTITC



EUROSMART



WILEY



EMOUSIN



NOKIA



vediohna

Introduction

- Les réseaux "sans fil" sont aujourd'hui omniprésents dans notre quotidien.
- Avec leurs évolutions, la sécurité est maintenant devenue plus qu'une simple fonctionnalité.
 - Quelles sont les solutions de sécurité aujourd'hui proposées et déployées ?
 - Quelles sont les solutions en cours de développement ?
 - Quelle confiance peut-on leur accorder ?

- Parcours :
 - Mastère en Sécurité des Systèmes d'Information de la FST de l'Université de Limoges
 - Ingénieur expert en sécurité des réseaux sans fil chez Bluesafe depuis plus de trois ans
 - Chef de projet sécurité des réseaux sans fil Bluesafe
 - Intervenant dans le Master en Sécurité des Systèmes d'Information à Limoges
- La société Bluesafe

Références :

- **Concevoir**
 - Conseil et expertise technique
 - Définition de politique de sécurité
 - Définition de schémas directeurs
 - Formation aux normes et principes d'architecture
- **Intégrer**
 - Étude de site
 - Déploiement de réseaux Wi-Fi multiservices WVoIP, WLAN et Work Spot
 - Sécurisation des accès nomades (WLAN, hot spot privés)
 - Transfert de compétences
- **Valider**
 - Tests intrusifs
 - Audit de sécurité
 - Audit de qualité de service (radio)
- **Maintenir**
 - Support proactif
 - Maintenance préventive et curative sur site
- **Gérer**
 - Opérer des réseaux Wi-Fi (Hot spot sur mesure,...)

- Parcours :
 - Centre d'Evaluation de la Sécurité des Technologies de l'Information (3 ans)
 - Postdoc au sein de l'*Information Security Group* du Royal Holloway, University of London
 - Maître de Conférences en Informatique à l'Université de Limoges
- Vice-président du GT 11.2 de l'IFIP *Pervasive System Security*
- Impliqué dans une douzaine d'évènements internationaux en sécurité

Plan de la présentation

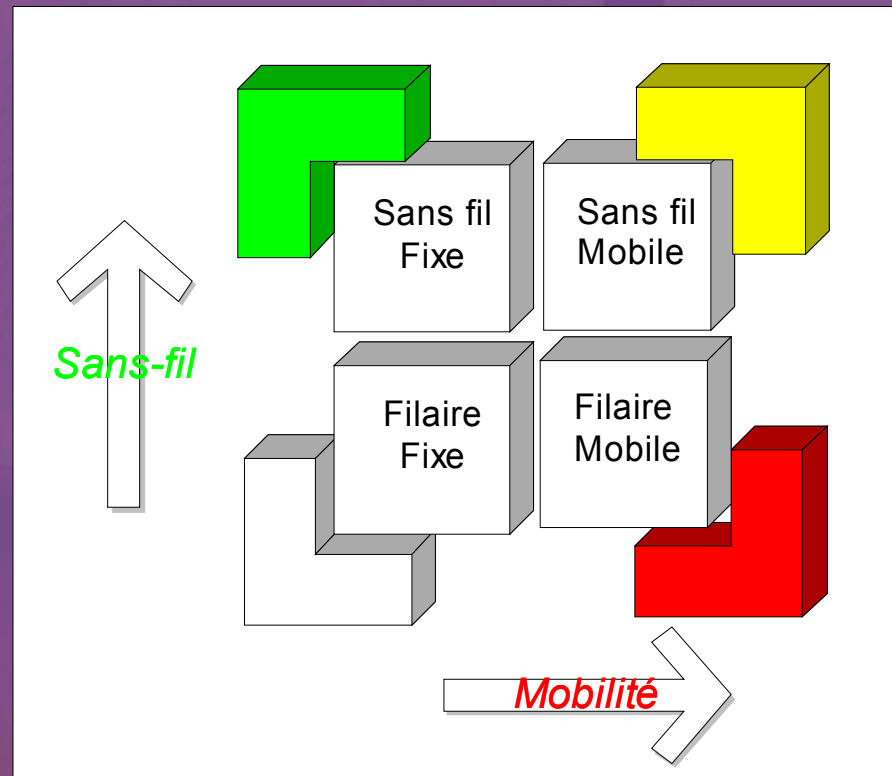
- La sécurité dans les réseaux traditionnels
- Un début de mobilité dans les réseaux traditionnels et la sécurité
- La sécurité dans le cadre de la mobilité lié à l'apparition des réseaux sans fil
 - Sécurisation du Wi-Fi / WLAN
 - Sécurisation de réseau "guest"
 - Un exemple concret : l'entrepôt
 - La géolocalisation des menaces
- Vers une mobilité totale et sans infrastructure : le réseau ad hoc pur
 - Présentation des solutions en cours d'élaboration dans les laboratoires de recherche
- Conclusion et Perspectives

Qu'est-ce qu'un réseau ?

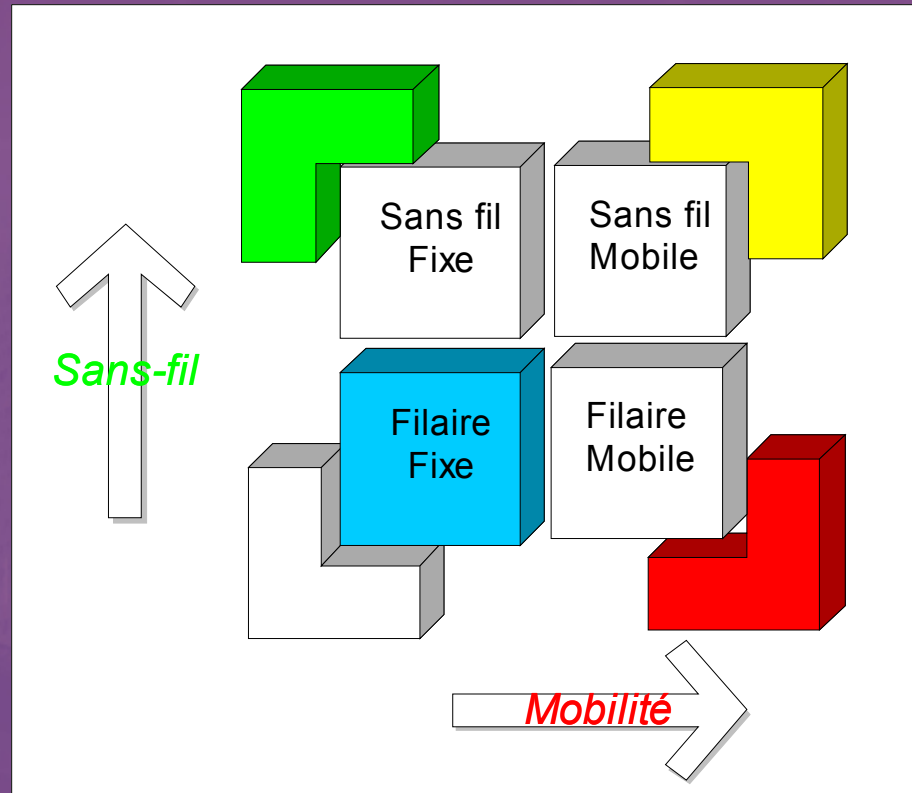
- Interconnexion de machines autonomes dans le but :
 - de partager des ressources :
 - matérielles
 - logicielles
 - de l'information
 - d'échanger des données :
 - communication (service de messagerie, téléphonie sur IP, ...);
 - production (écriture et soumission de rapport, ...).
- bref, de **travailler de manière collaborative** (contribuer à produire à un travail commun).

Classification des réseaux

- Critères :
 - **Mobilité** : fixe et mobile ;
 - **Type de liaison** : filaire et « sans fil ».

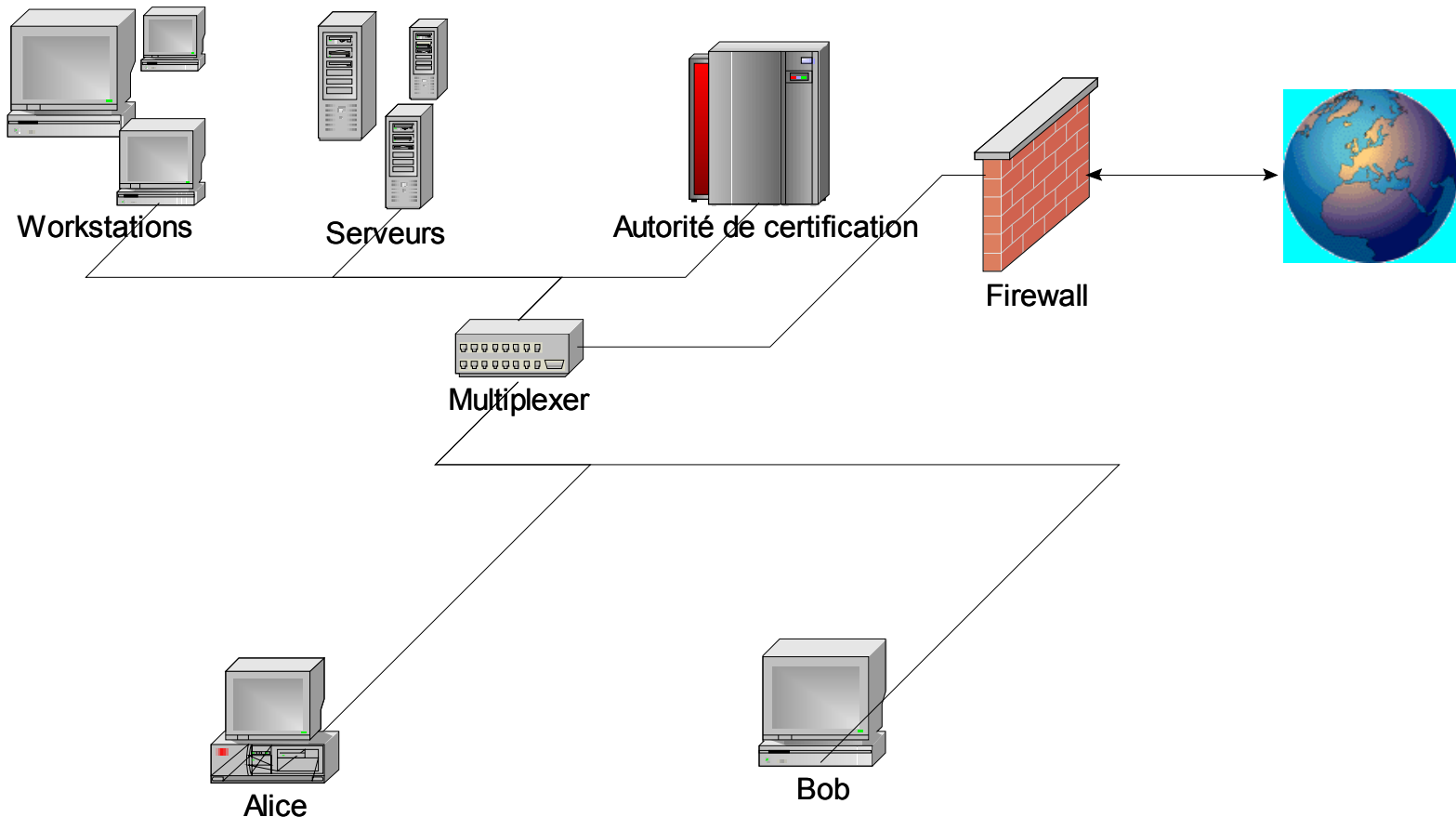


Les réseaux traditionnels



Les réseaux traditionnels

- Ce type de réseau utilise uniquement du filaire.

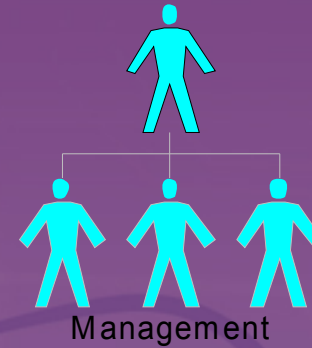


Sécurisation du réseau : **définir la frontière**

- Contrôler les accès au réseau :

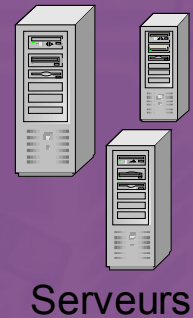
- **définition d'une identité** pour :

- chaque serveur ;
 - chaque utilisateur.



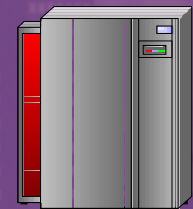
- **affectation d'un rôle** :

- appartenance d'un utilisateur à un groupe ;
 - distribution des responsabilités entre utilisateurs ;
 - affectation des services fournis par les machines ;
 - ...



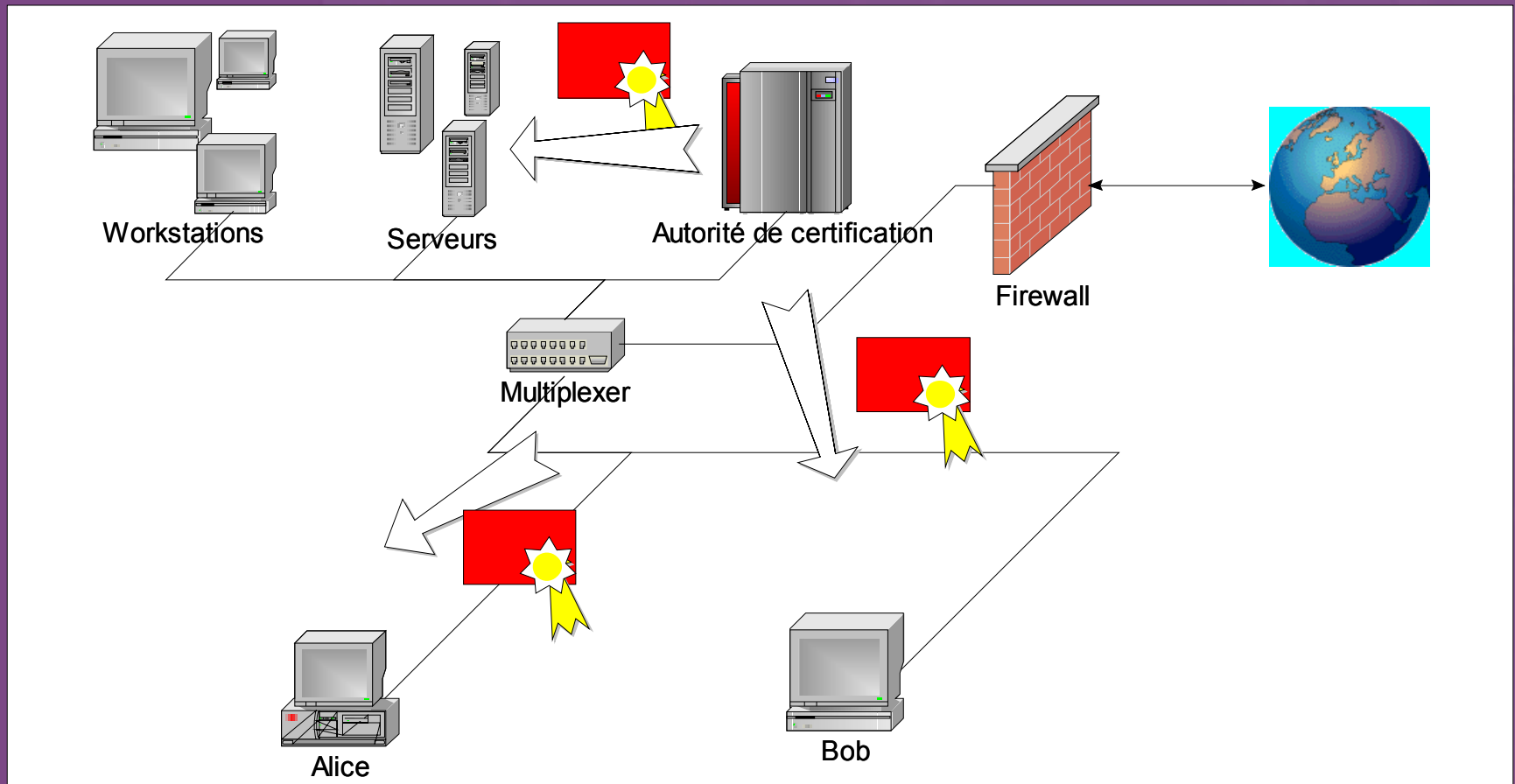
- **Définition d'une « frontière » pour le réseau**

- utilisation de certificats ;
 - mise en place d'une autorité de certification.



La frontière dans un réseau traditionnel

- Diffusion et utilisation de certificats.

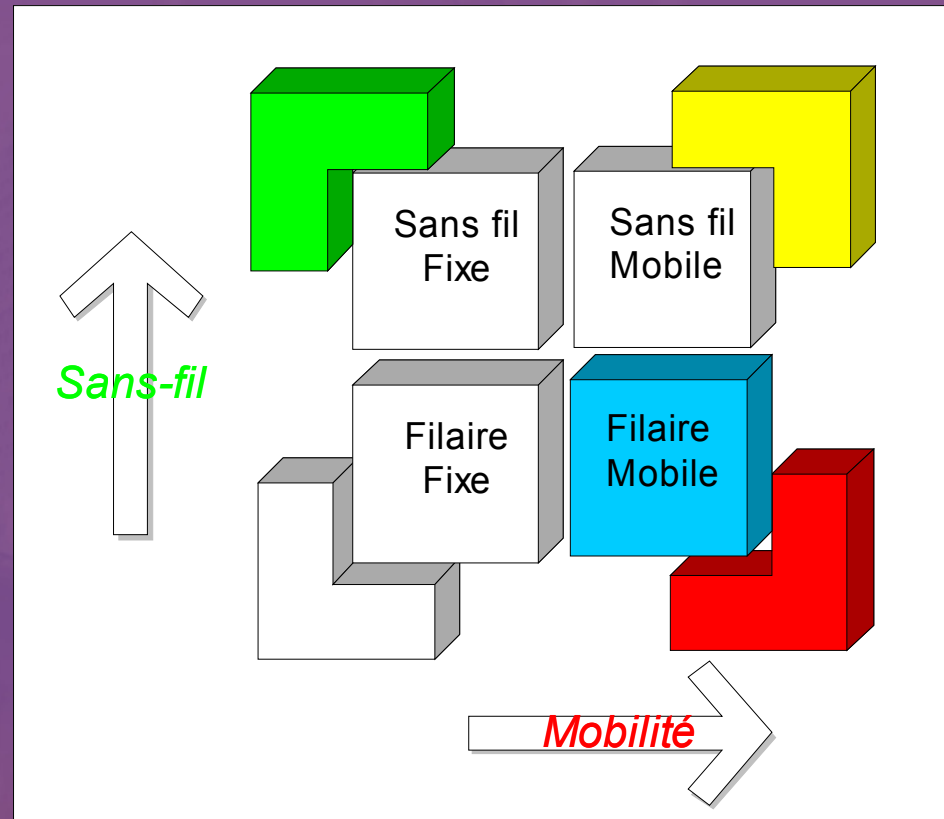


Quelques services de sécurité supplémentaires

- **Sécurité des identités** versus **Sécurité des comportements** :
 - « *Toutes les personnes en prison ont une carte d'identité !* »
Nicolas Prigent, Thomson R&D.
- Mécanismes de sécurité contre des attaques externes mais aussi des attaques internes !
 - Firewall (DMZ, etc.)
 - Antivirus
 - IDS, NIDS

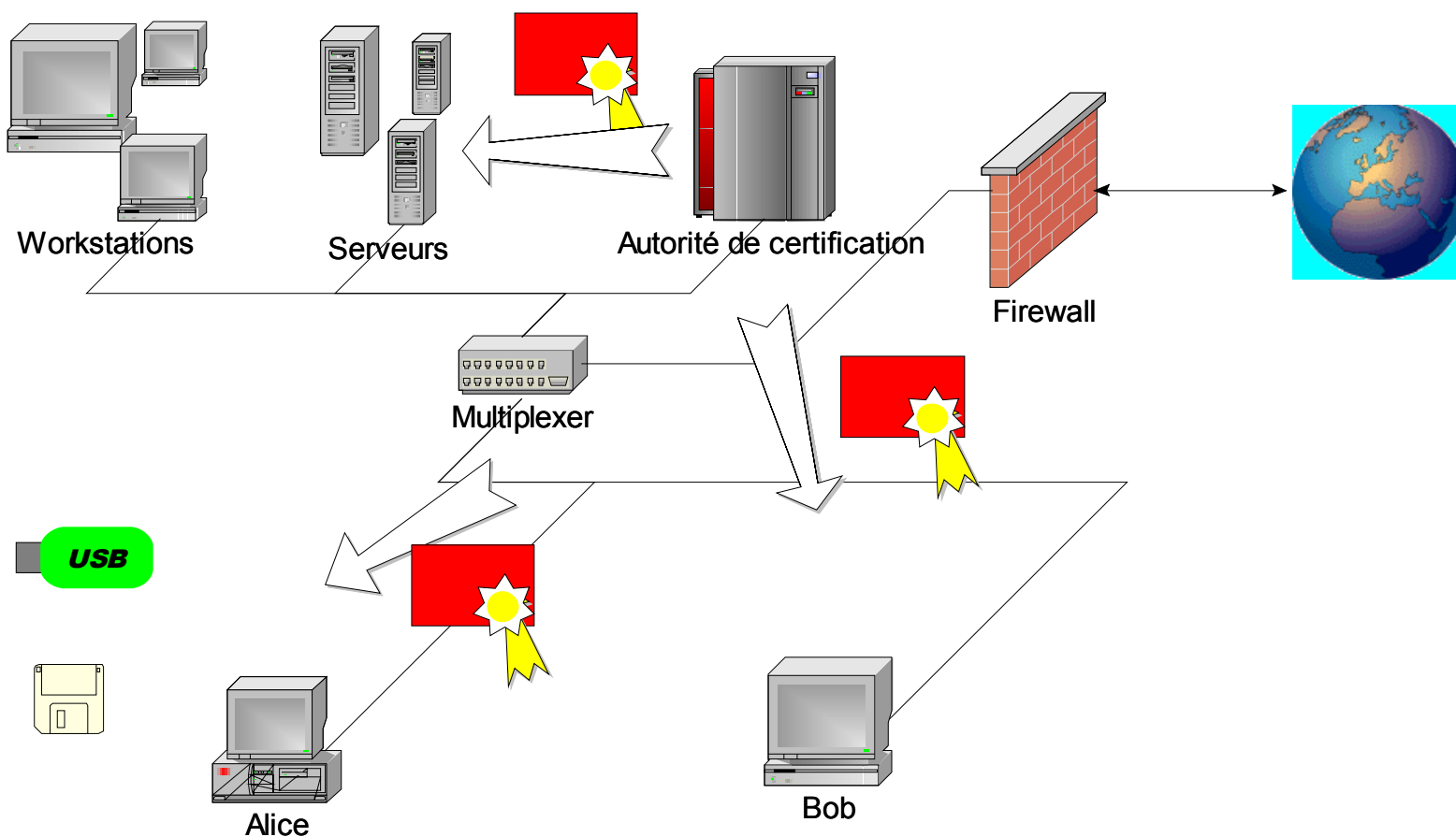
La mobilité dans les réseaux traditionnels

- Une envie et un besoin des utilisateurs...
...le cauchemar de l'administrateur



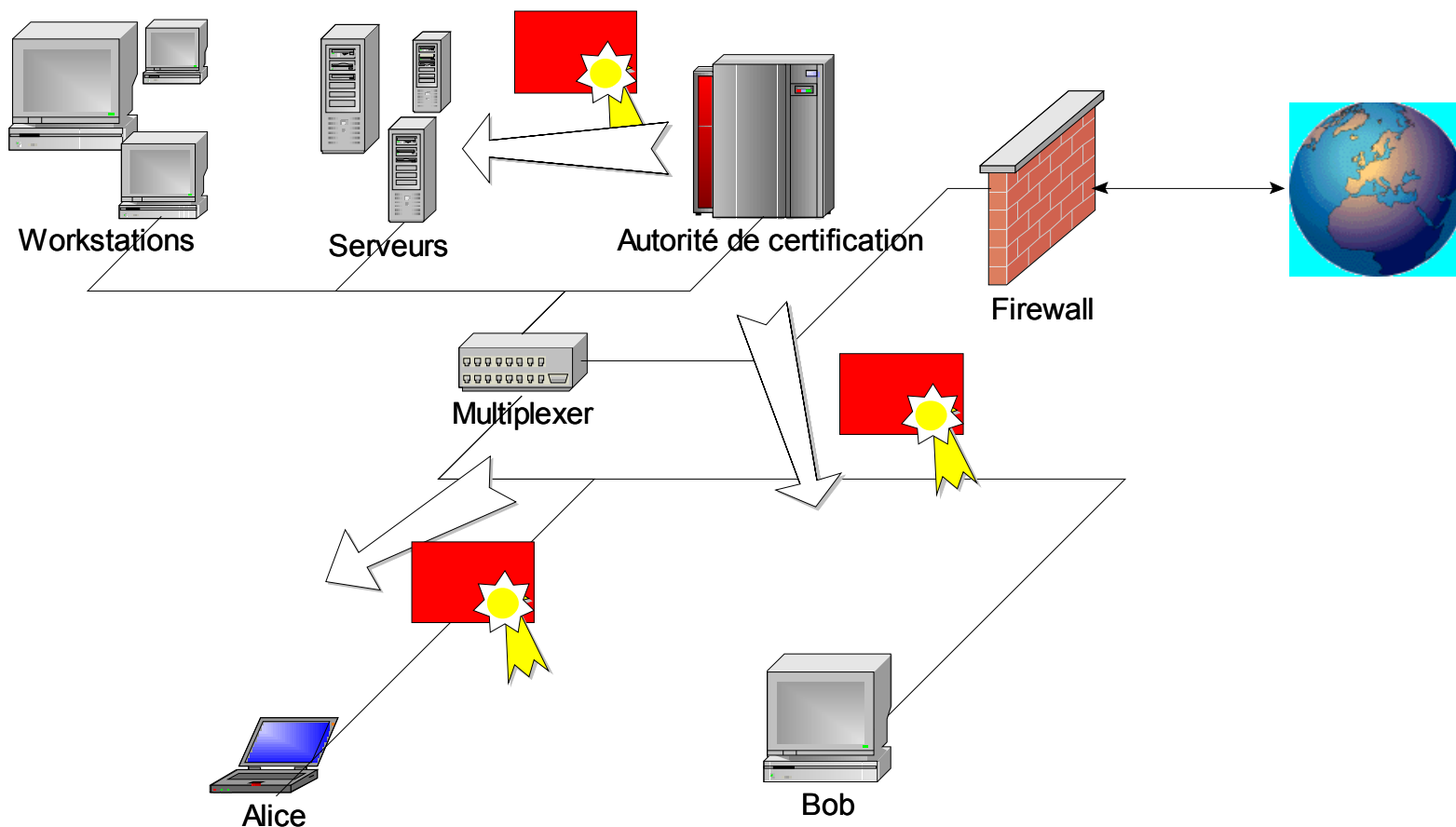
Mobilité : les données

- L'utilisateur emporte **avec lui** ses données sur un support amovible à l'extérieur du réseau.



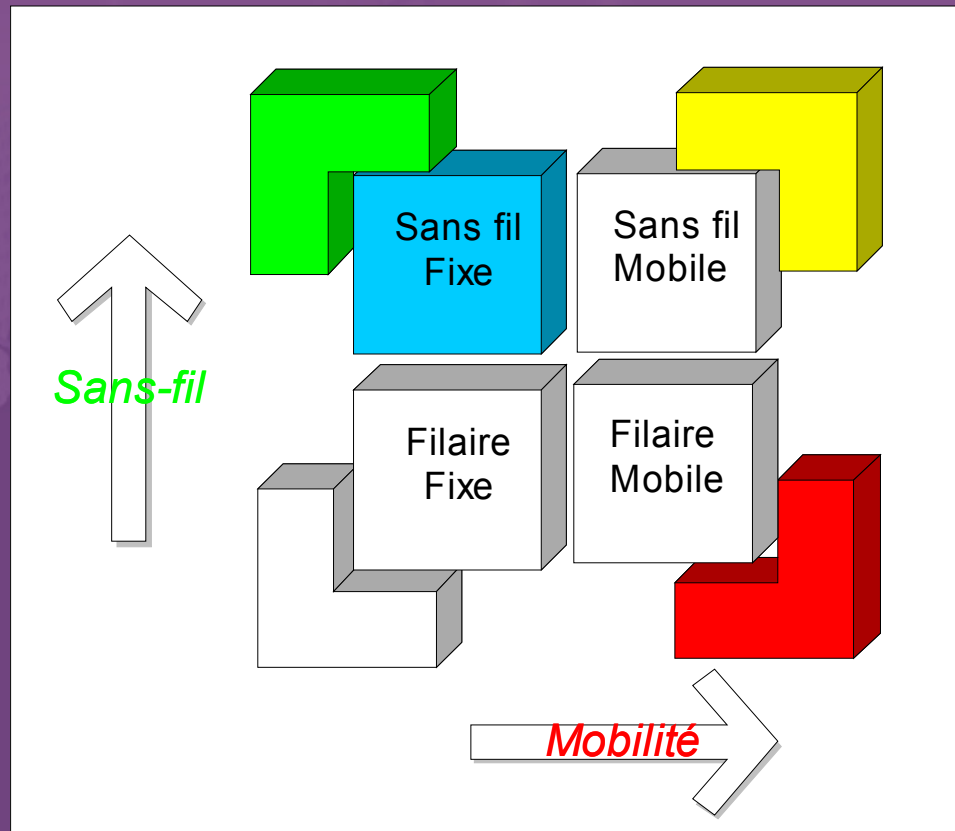
Mobilité : le contrôle

- L'utilisateur emporte **avec lui** sa machine à l'extérieur du réseau (données + processus).



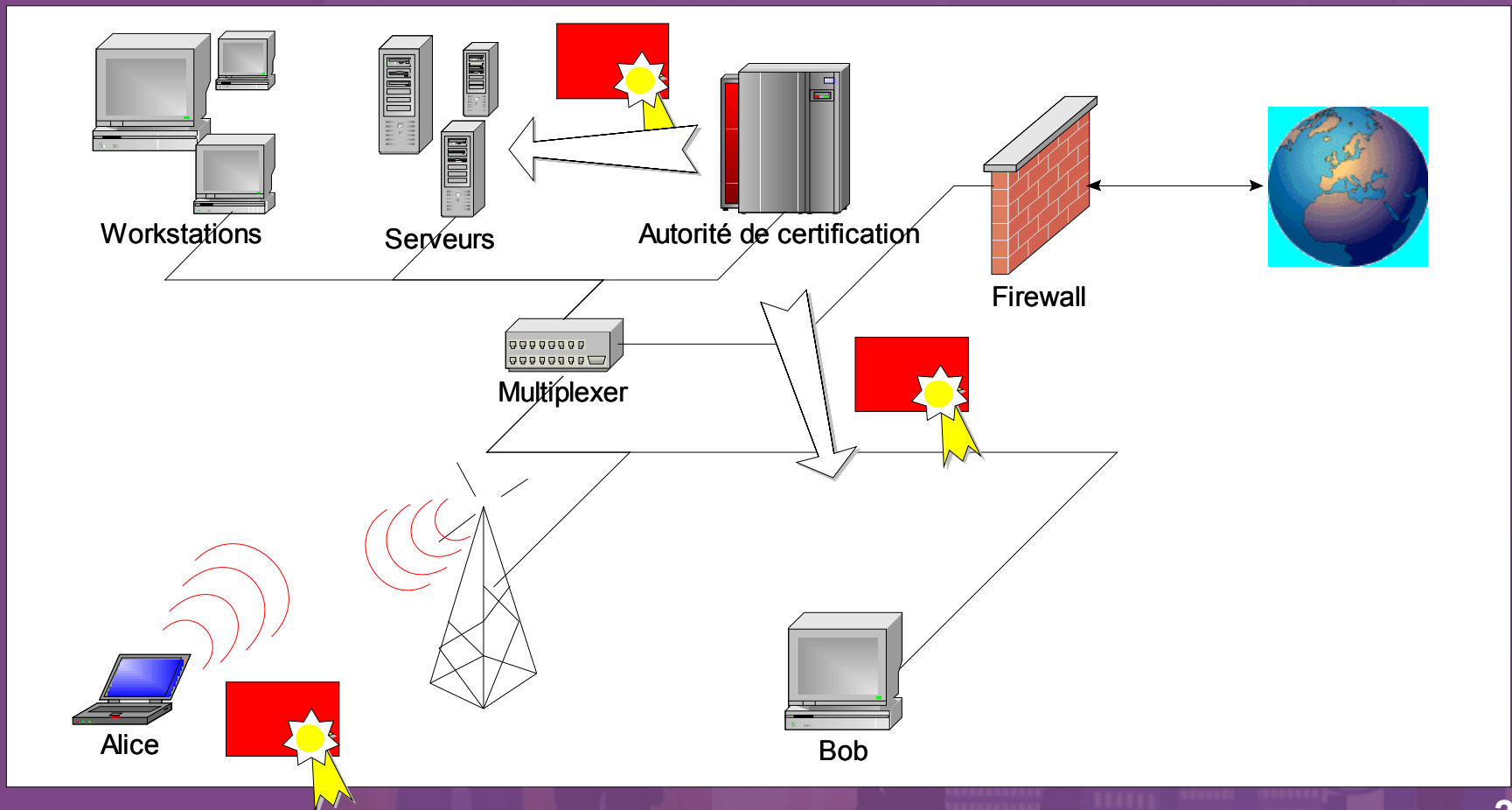
Le sans fil : supprimer les câbles

- Certaines liaisons sont remplacées par des liaisons sans fil.



Le sans fil : supprimer les câbles

- L'utilisateur accède au réseau par une liaison sans fil (WiFi, Bluetooth, GSM/GPRS, ...)



- Convergence des besoins, mutualisés en sécurité
 - Accès sécurisés : collaborateurs au LAN, Téléphonie mobile, Terminaux métiers logistiques, Terminaux métiers ventes (accès type WLAN)
 - Accès contrôlés des visiteurs à Internet : HotSpot privé (accès invité)
 - Géolocalisation : Localisation des menaces

- Risques :
 - De part la nature immatérielle du support physique :
 - Intrusion réseau
 - Interception des données
 - Dénî de service
- Solutions :
 - 802.11i
 - Sécurisation de l'accès au média : authentification
 - Sécurisation du média : chiffrement robuste
 - WIPS
 - Blocage de Dénî de service

- Indépendant de la norme radio : compatible avec 802.11a, 802.11b, 802.11g et 802.11n !
- 802.1x – EAP :
 - Processus d'authentification du client se déroule dans un tunnel sécurisé : protège l'échange et authentifie le serveur d'authentification
 - Protocole EAP est lui-même un protocole générique qui permet d'encapsuler toute méthode d'authentification : EAP-TLS, PEAP, EAP-TTLS, EAP-FAST
- RSN :
 - Robust Security Network : définit la gestion de la distribution et la dérivation des clés entre les APs et les clients
- AES-CCMP :
 - Chiffrement basé sur AES en mode CCM
 - CCM combine Counter Mode et CBC-MAC pour garantir l'intégrité et interdire les re-jeux des trames chiffrées

- Dans 802.11i
 - Pre-Authentication
 - Key Caching
- En attendant 802.11r
 - Fast Roaming
 - Proactive Key Caching
 - Opportunistic Key Caching

- Portail Captif HTTPS (solution dédiée aux visiteurs)
 - Une solution d'authentification simple avec aucune configuration au niveau du client
 - Prise en compte de l'Accounting (gestion du temps)
 - Firewall pour contenir les flux, et limiter les accès
 - Sécurise le système d'information de l'entreprise
 - Logs et User Tracking impératif (LCT)
 - Isole du reste du LAN



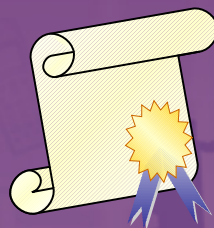
L'entrepôt :

– Composants de sécurité :

- Un pistolet code barre : EAN128, etc.



- Un certificat : EAP-TLS



- Un serveur radius : IAS, SBR, ACS

- Des points d'accès



- Contrôleur de mobilité



- Applicatif sécurisé : SAP, AS400

- Sondes monitoring



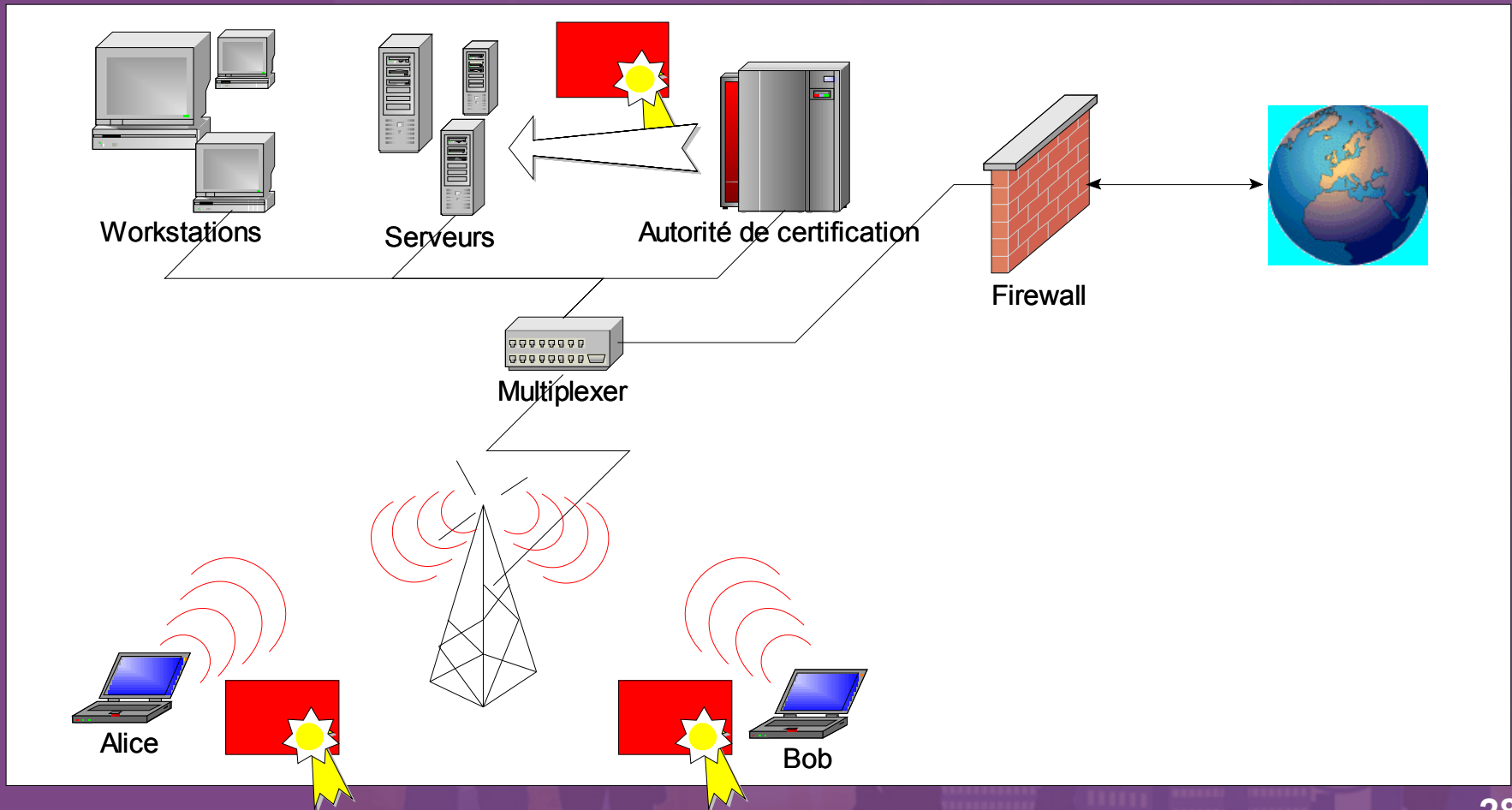
- Géolocalisation



- Profiter de l'architecture mise en œuvre : Mettre le point d'accès en mode mixte « borne/sonde » de manière permanente
- IDS/IPS :
 - Points d'accès et périphériques pirates
 - Des dénis de service, ...
- Géolocalisation :
 - Des tentatives d'intrusions,
 - Des systèmes non autorisés,
 - Des dénis de service, ...

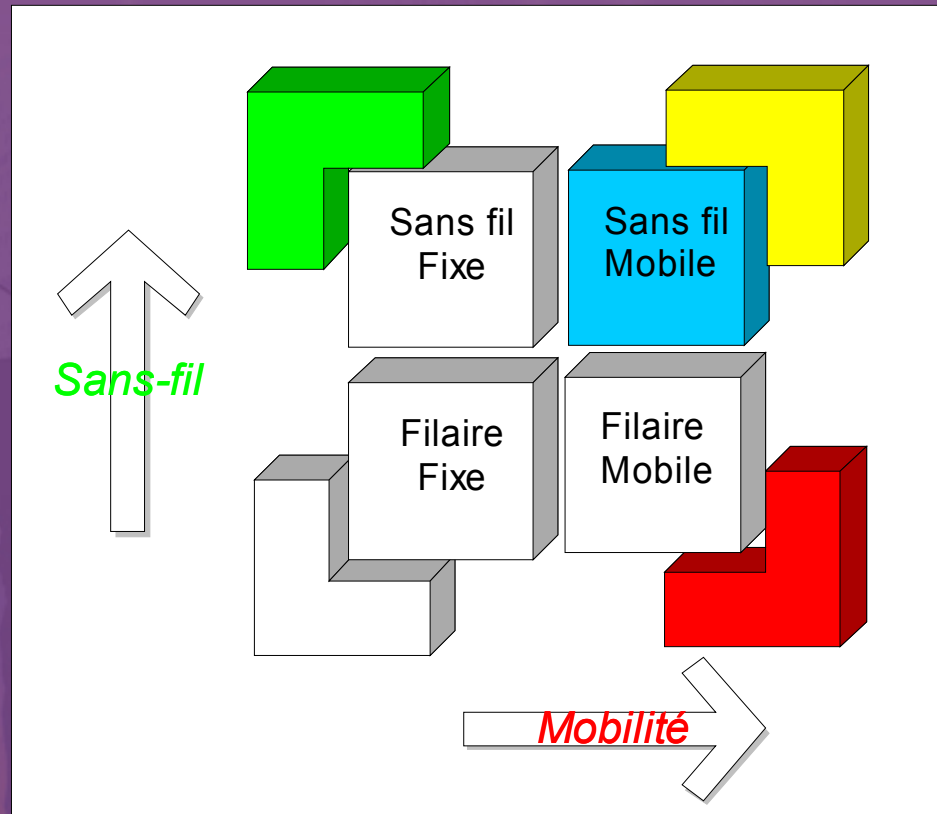
Le sans fil : avec infrastructure

- L'utilisation du sans fil se généralise et permet les échanges entre utilisateurs purement sans fil.

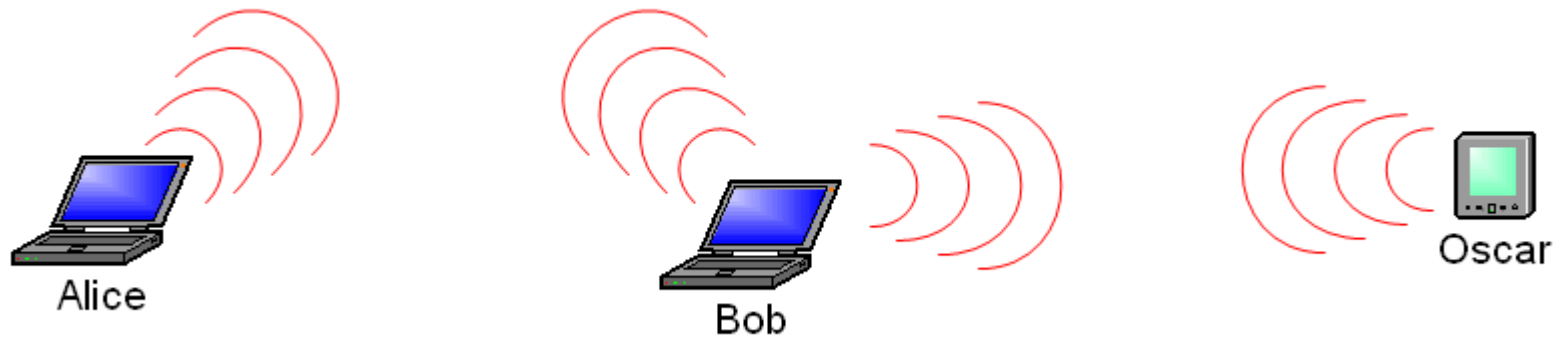


Généralisation des réseaux sans fils

- Les structures physiques du réseau se dématérialisent ;
- les postes sont mobiles ;
- *la frontière du réseau reste identique.*



Le sans fil : réseau ad hoc



Le sans fil : ...avec infrastructure

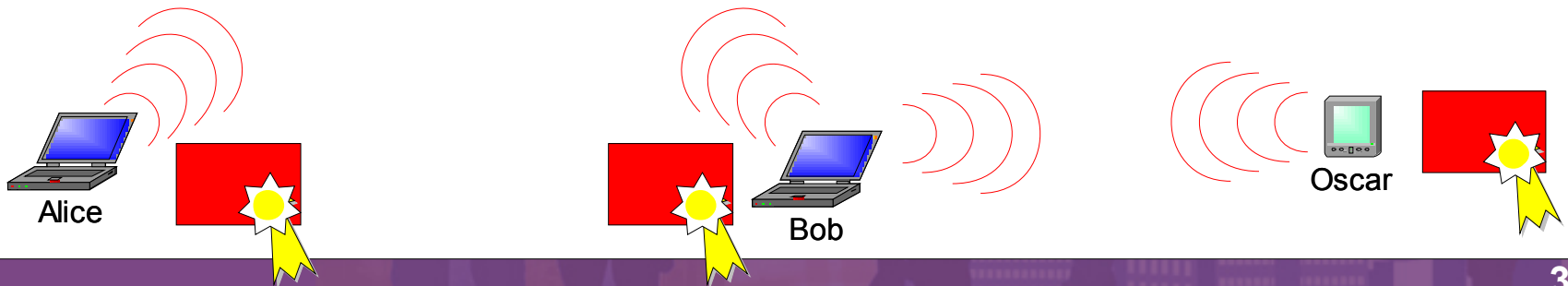
- *L'infrastructure est conservée par l'utilisation de certificats hérités d'une structure !*

c'est le modèle qui est souvent proposé en tant que réseau ad hoc sécurisé ;

Les noeuds du réseau doivent obtenir un certificat auprès d'une organisation commune (la frontière du réseau ad hoc est contrôlée par cette organisation) ;

Processus lourd à mettre en oeuvre

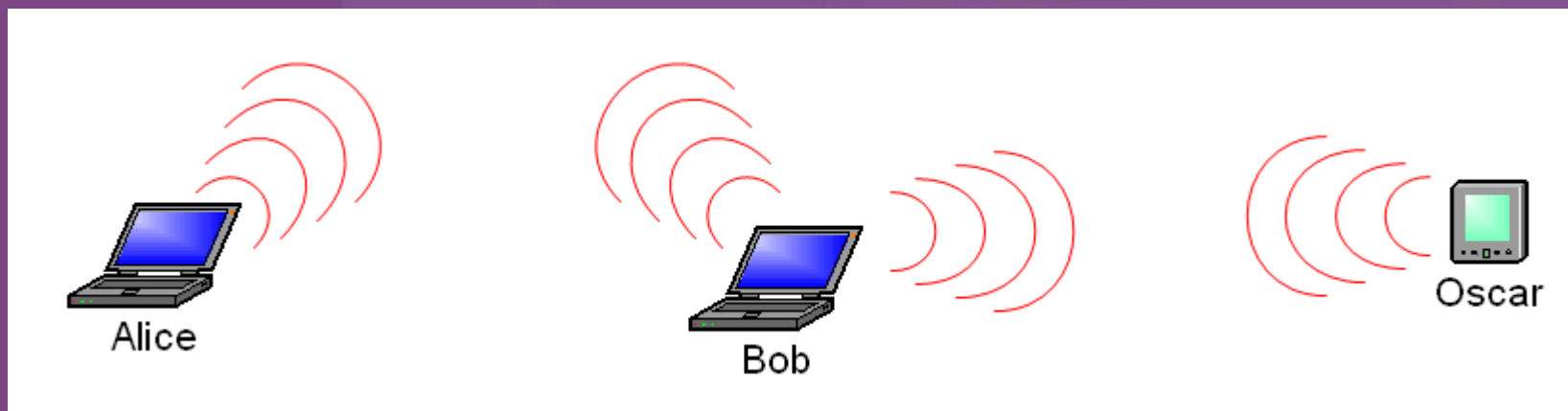
Ceci n'est pas un réseau **purement** ad hoc



Le sans fil: ...sans infrastructure

- Plus d'infrastructure...

Mais, où est la frontière ?



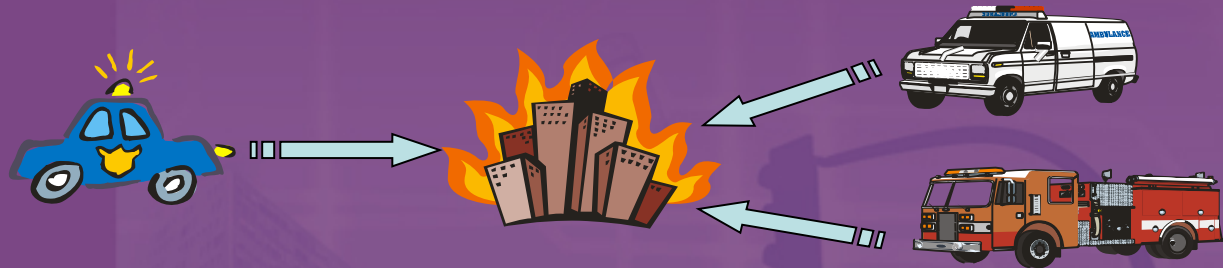
→ C'est le réseau ad hoc pur

Le réseau ad hoc pur

- Une partie de l'activité recherche d'XLIM :
 - Les réseaux sans fils haut débit
 - La sécurisation de ces réseaux ad hoc purs
 - Travaux réalisés pour partie au sein du projet ANR ARA “Sécurité des Systèmes embarqués et Intelligence Ambiante” SARAH
 - LaBRI, LITIS, VALORIA, XLIM

Cas d'utilisation actuellement visés

- Etats de crise : attentats, séismes, ...

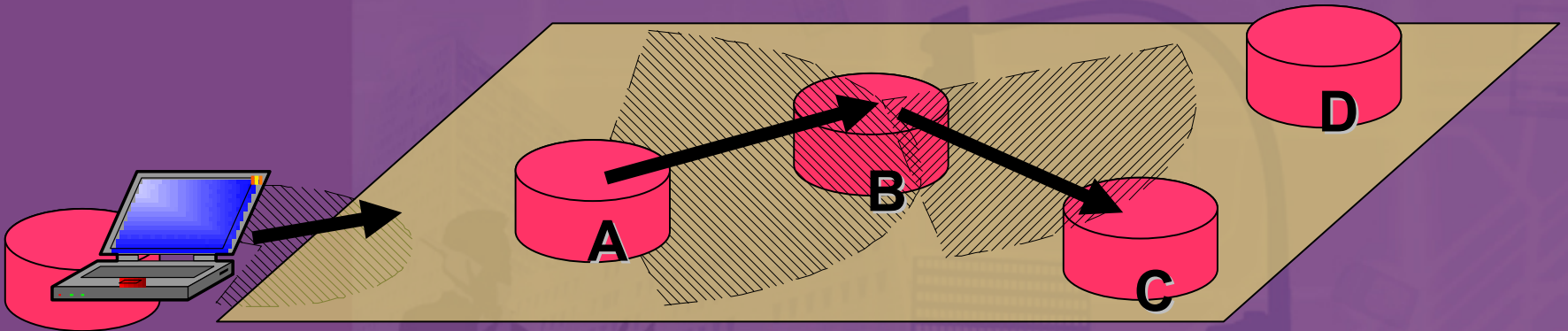


- Dans ces situations, plus d'infrastructure !
Comment faire communiquer les secours ?



Quelques problématiques des réseaux ad hoc purs

- La portée radio étant limitée, on passe par des noeuds intermédiaires



- **Problème** : B peut être égoïste, malveillant, défectueux

Conjecture sur l'évolution des réseaux

- *Le nomadisme est une perspective incontournable à laquelle la sécurité devra s'adapter !*
- **Notre objectif : Transposer les possibilités d'un réseau traditionnel dans un réseau purement ad hoc afin de supporter du travail collaboratif de manière sécurisée.**

Récapitulatif de solutions de sécurités existantes

- Ce qui existe
 - les communications sont abondamment traitées (GSM, WiFi et WPA, Bluetooth, ...) ;
 - les transactions le sont aussi (gestion bancaire, manipulation de BD, achat, ...).
- **Les limites**
 - les solutions proposées s'appuient toujours **sur une infrastructure** : le réseau de l'opérateur GSM par exemple.
- *Comment se passer de toute infrastructure et proposer une architecture autonome ?*

Les contraintes et réponses

- **Les contraintes des technologies de communication**
 - un réseau ad hoc subit de nombreux événements ;
 - impossibilité d'utiliser directement l'abstraction TCP/IP ;
 - **débit limité des liaisons** par rapport au filaire ;
 - durée de vie du réseau liée à la présence de ses noeuds.
- **Les réponses**
 - chaque noeud doit être identifié de manière globale pour ce réseau (frontière) ;
 - chaque noeud doit participer à la vie du réseau
 - gérer le routage des messages entre les noeuds,
 - c'est-à-dire, **collaborer** avec les autres noeuds ;
 - le réseau doit être défini pour une durée déterminée.

La mise en oeuvre des réponses

- Cela passe par :
 - la mise en oeuvre d'une **plate-forme de confiance** dont l'objectif est l'organisation du réseau :
 - définition d'une identité pour le réseau et pour les noeuds ;
 - définition d'une frontière ;
 - définition et mise en application d'une politique de sécurité.
 - la **mise en oeuvre d'applications** dans ces réseaux à destination des utilisateurs : création de documents, partage d'informations, protection de contenu, communications, ...
- *La couche applicative exploite les mécanismes de sécurité offerts au niveau de la plate-forme de confiance.*

Les contraintes et réponses

- **Les contraintes liées aux noeuds du réseau**
 - utilisation de terminaux de faible puissance de calcul (l'autonomie et la puissance sont antagonistes) ;
 - utilisation d'environnement de développement logiciel standard
 - déploiement sur différents systèmes d'exploitations ;
 - interopérabilité entre les noeuds ;
 - acceptation du logiciel nécessaire au bon fonctionnement du réseau (garantie de protection du code vis à vis de l'hôte et vice-versa).
- **Les réponses**
 - utilisation d'algo. **coopératifs** légers et efficaces ;
 - choix d'une plate-forme de mobilité **portable** ;
 - utilisation d'un environnement d'exécution protégé et **facilement déployable** : la carte à puce

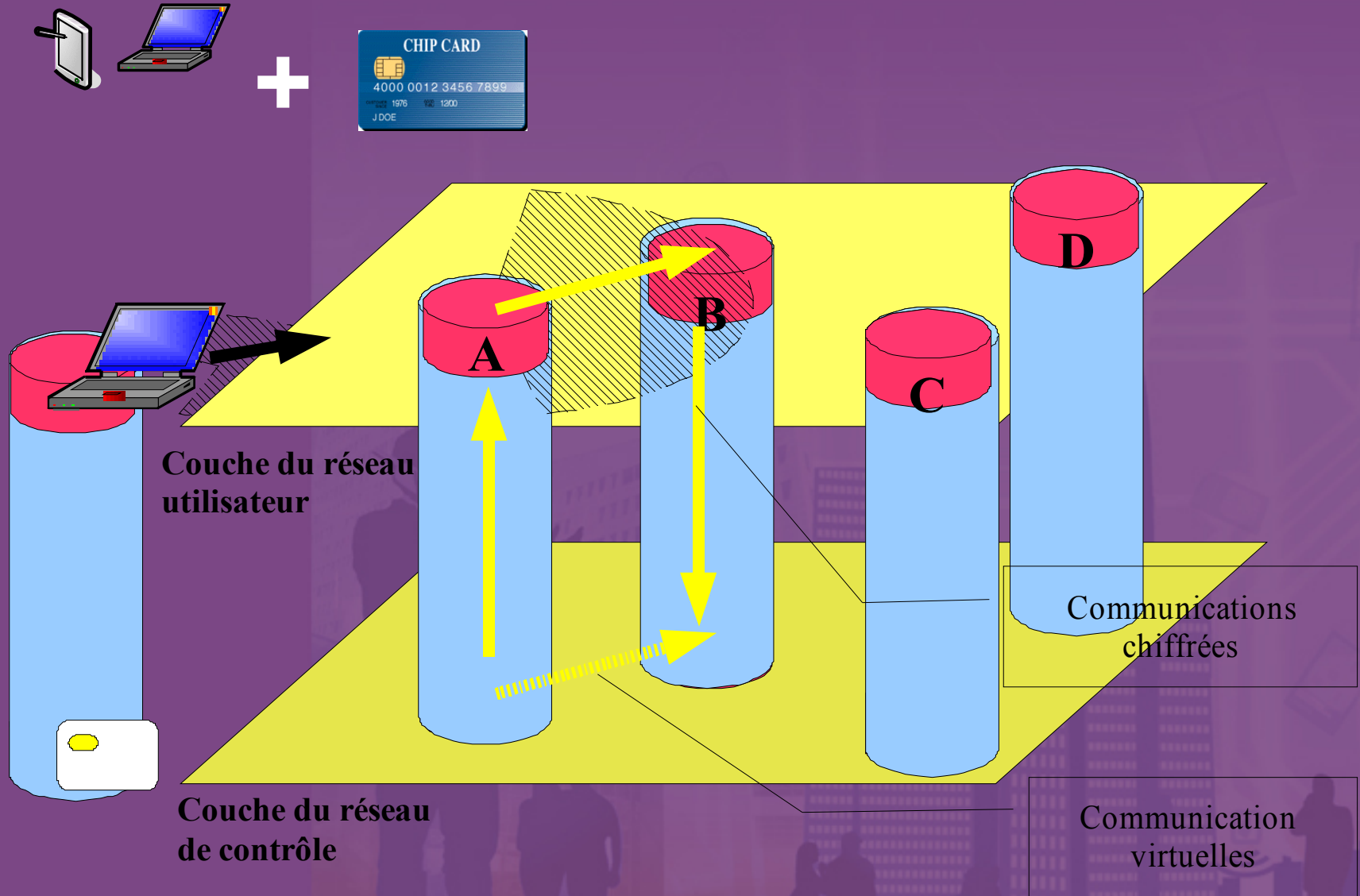
La plate-forme de confiance

- Elle est assurée via une **application distribuée** sur chaque noeud du réseau.
- Cette application doit s'exécuter de manière indépendante, transparente et sécurisée vis-à-vis du noeud :
 - **l'utilisateur** ne doit pas pouvoir modifier ou espionner le code à son avantage ;
 - **le code** ne doit pas pouvoir modifier et espionner les traitements exécutés sur le noeud.
 - **La confiance que l'on peut avoir dans la plate-forme repose entièrement sur le respect et la garantie de ces deux conditions.**
- La seule solution : adjoindre un processeur sécurisé à chaque noeud qui effectuera ces traitements.

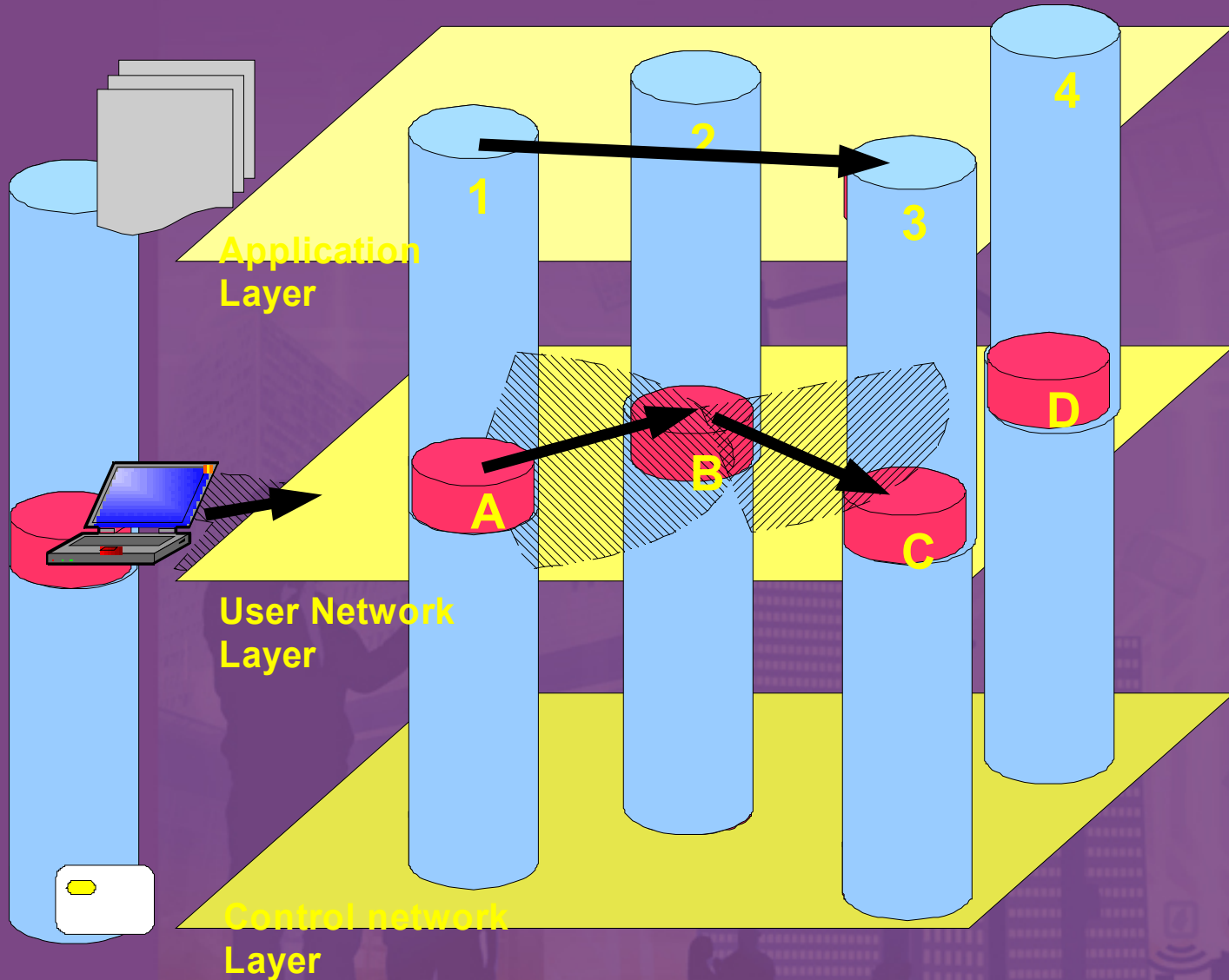
Le choix du processeur sécurisé

- La technologie candidate actuellement disponible facilement est la **carte à puce**.
- Ses avantages simplifient notre mise en oeuvre :
 - possibilité de **communiquer de manière sécurisée** et indépendante de l'utilisateur ;
 - création d'une **identité unique, inaltérable et inconnue** de l'utilisateur pour le noeud et le réseau ;
 - possibilité de définir un **mécanisme d'horodatage** simplifié pour les opérations dans le réseau ;
 - **incitation et contrôle de la collaboration** des noeuds (utilisation d'un système de rétribution géré facilement par la carte à puce) ;
 - **hypothèses simplificatrices** pour les algos de crypto employés pour les couches applicative et de confiance.

Architecture de MADNESS



Un échange dans MADNESS



Création, terminaison et durée de vie du réseau, etc.

- Le plus compliqué reste est de créer **dynamiquement** des réseaux, dans des buts bien précis, qui résistent au partitionnement, etc.
- À lire bientôt dans nos publications ;-)
 - *MANETS: an exclusive choice between use and security?*
P-F Bonnefoi, D. Sauveron et J. H. Park.
 - *Mobile AD hoc Network with Embedded Secure System.*
E. Atallah, P-F. Bonnefoi, C. Burgod et D. Sauveron.

Conclusion et Perspectives

- La technologie offre à l'utilisateur toujours plus de souplesse dans l'utilisation, de mobilité, etc. → nomadisme
- Les réseaux ont une frontière de plus en plus mobile.
- La sécurité doit et devra être intégrée à tous les produits connectés.
- Elle doit être pensée depuis l'étape de conception.



Questions ? Commentaires ?



Remerciements

- À Pierre-François Bonnefoi (XLIM), Maître de Conférences, auteur de la plupart des illustrations utilisées dans cette présentation

