INSTITUT
Mines-Télécom

Gestion des données respectueuse de la vie privée

Maryline LAURENT
Resp. Equipe R3S, CNRS SAMOVAR UMR5157
Cofondatrice de la chaire Valeurs et politiques des informations personnelles

TELECOM SudParis

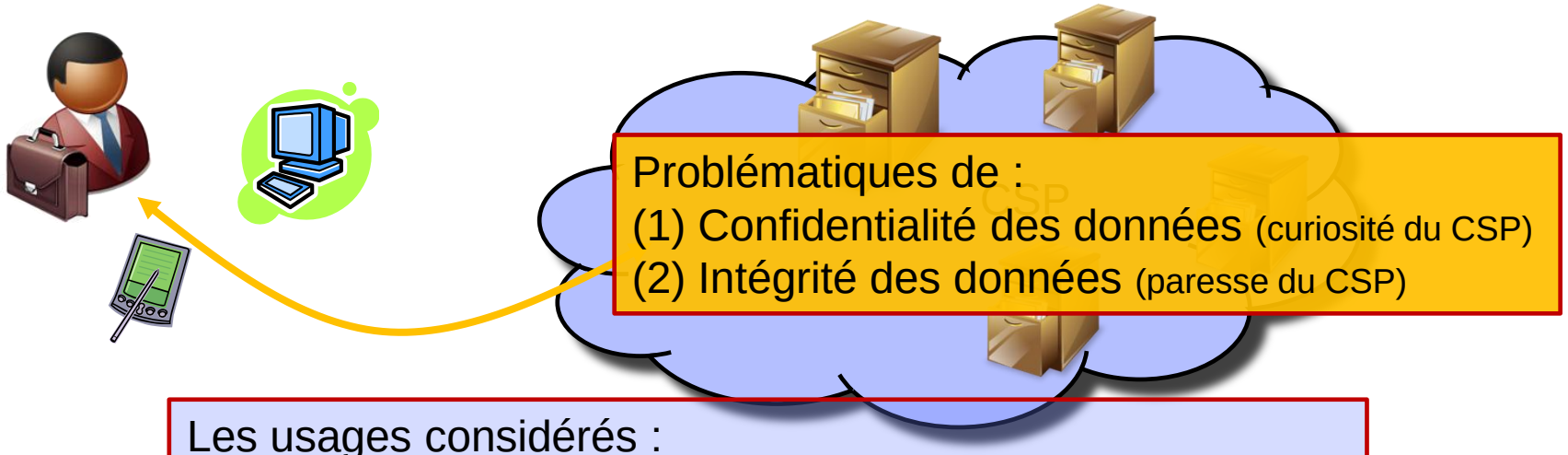
Contenu de présentation

- **2 cas d'usage passés en revue :**
  - **Cloud computing (storage)**
  - **Réseaux domestiques**

- **Travaux réalisés dans le cadre de la chaire de l'Institut Mines-Télécom Valeurs et politiques des informations personnelles, de projets collaboratifs et de projets de recherche**

Cloud computing (storage)

Stockage de données dans un cloud



Problématiques de :
(1) Confidentialité des données (curiosité du CSP)
(2) Intégrité des données (paresse du CSP)

Les usages considérés :
(a) Backup : seul le propriétaire récupère ses données
(b) Partage de données : accès fourni à un autre utilisateur

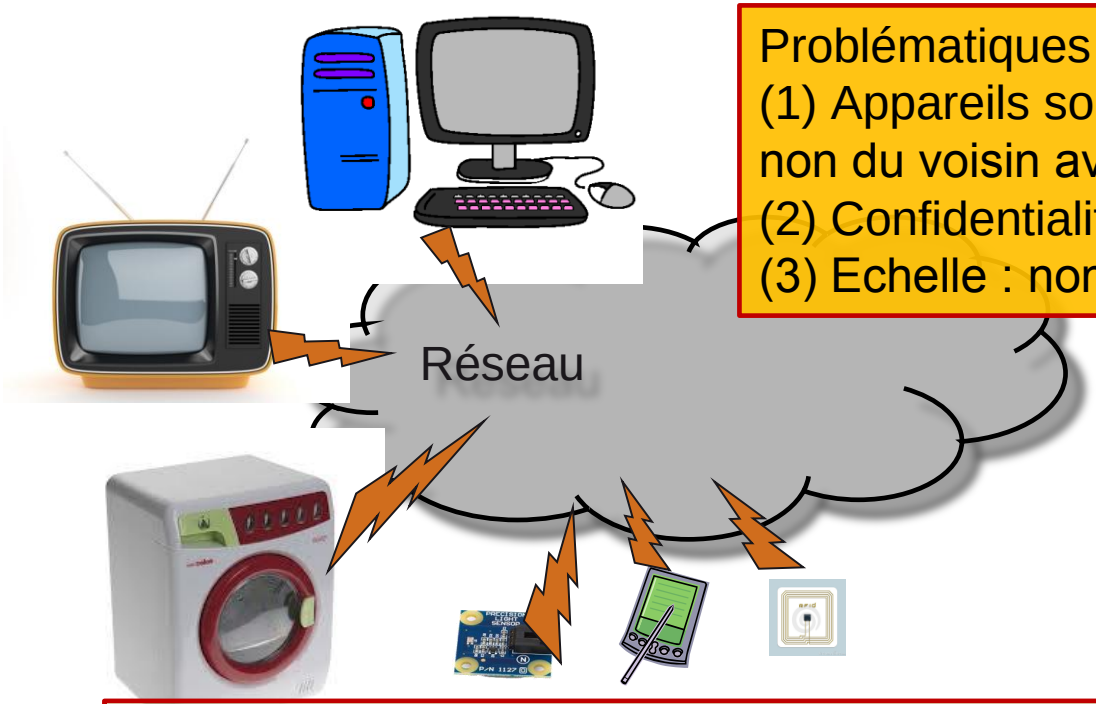
Solutions apportées - Projet FUI 11 ODISEA :
(1a-1b) Chiffrement par le propriétaire de ses contenus avec accès à un tiers sous contrôle
(2) Preuve de possession apportée par le CSP au propriétaire
Sous des contraintes de performances (capacités des terminaux, facilité d'exploitation, bande passante…)

Résultats

- 3 publications dans des conférences de haut niveau
- Démonstrateur de toutes les contributions réalisé avec OpenStack
- Mesure de performances

Réseaux domestiques

Réseaux domestiques

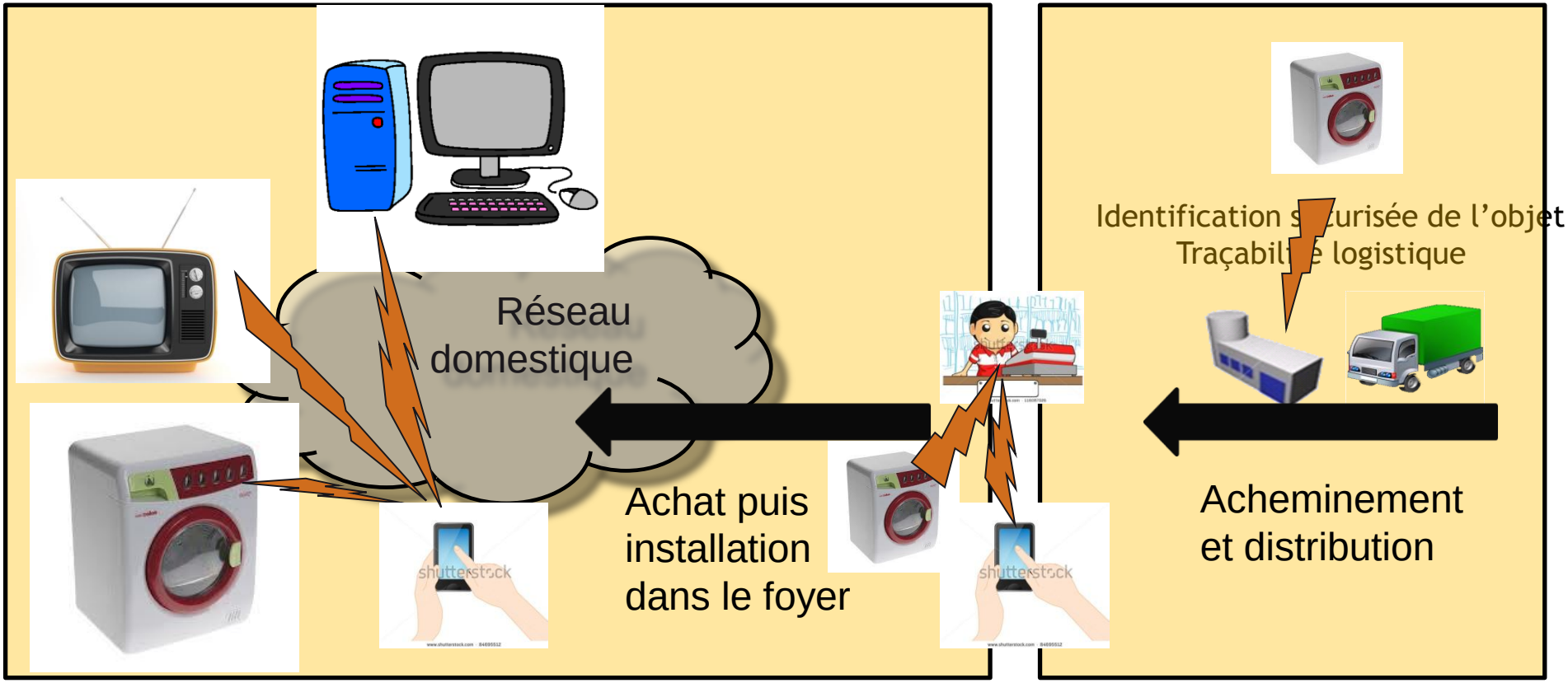


Problématiques de sécurité et de vie privée :
(1) Appareils sous contrôle du propriétaire et non du voisin avec des problèmes d'appairage
(2) Confidentialité des échanges entre appareils
(3) Echelle : nombre d' objets très important

Solutions apportées :
Protocoles de sécurité, non traçables, passant à l'échelle, résistants aux attaques classiques de sécurité

Sous des contraintes de performances (capacités des terminaux, facilité d'exploitation, bande passante…)

Exemple plus concret d'usage



Avantages : Traçabilité sous contrôle, sécurité et vie privée respectée, support du SAV

Résultats

- 2 brevets sur l'authentification mutuelle légère, dont un basé sur le cryptosystème asymétrique NTRU
- 7 publications : 2 articles de revue et 5 articles de conférence
- Une étude de maturation (OMTE) en cours par Digitéo
- Nomination au prix Fibre de l'innovation 2013

- Applicables à d'autres contextes : Smartgrid, IoT…

Conclusions

Conclusions

- **Travaux riches autour des technologies et techniques sur la protection des données personnelles**
- **Animations proposées sur ces sujets**
  - Rencontres de la chaire Valeurs et politiques des informations personnelles
  - Action CNRS SSO du GDR ASR sur la « sécurité des petits Objets et Internet des objets »
- **Atouts de l'Institut Mines-Télécom et Télécom SudParis**
  - Compétences en cryptographie et mécanismes de sécurité permettant d'élaborer des protocoles de sécurité respectueux de la vie privée
  - Propriété intellectuelle : démarche brevets bien rôdée