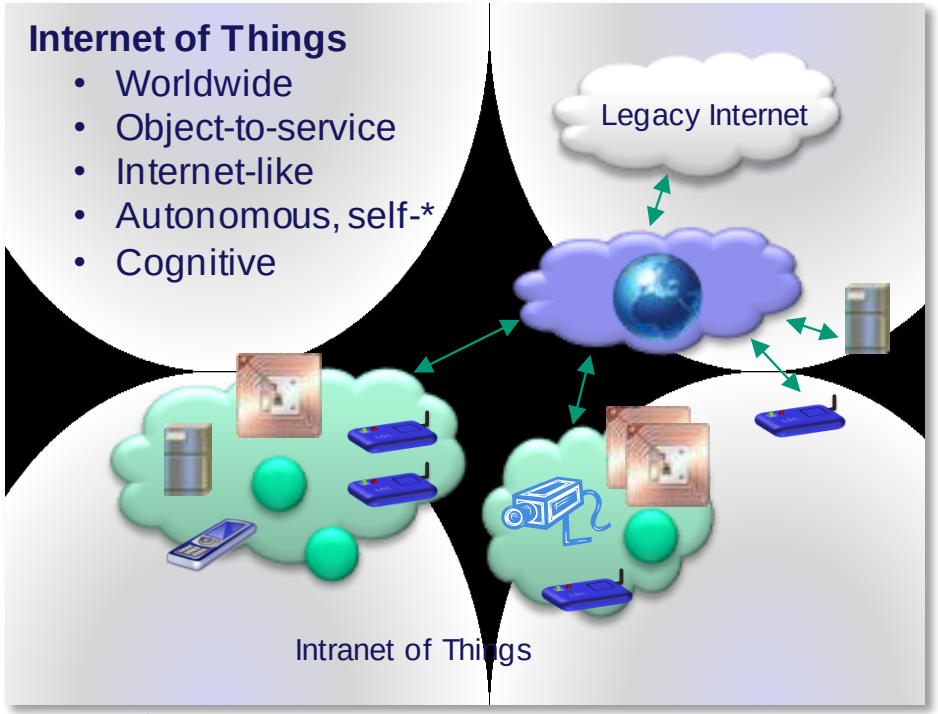
INSTITUT
Mines-Télécom

Vie privée dans l'Internet des Objets
Travail s'inscrivant dans la chaire « Valeurs et Politiques des Informations Personnelles »

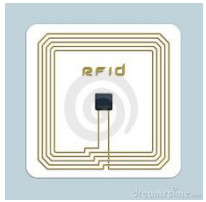
MINES Albi-Carmaux · MINES Alès · MINES Douai · MINES Nantes · MINES ParisTech · Ecole Nationale Supérieure des Mines Saint-Etienne · TELECOM Bretagne · TELECOM Ecole de Management · TELECOM ParisTech · TELECOM SudParis · EURECOM · TELECOM Lille · MINESnancy

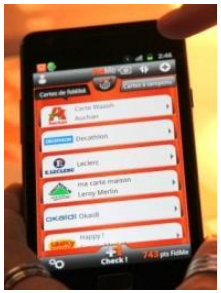
Internet des objets

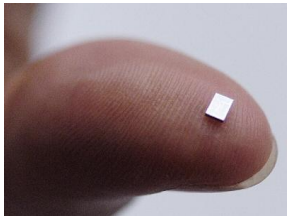


(source : Thèse de Y. Ben Saied)

- **Technologies multiples : RFID, capteurs, NFC…**







(source : numerama.com)

- **De nombreux usages : santé, domotique, transport, logistique…**

Au-delà de la sécurité, des risques et des besoins pour la vie privée…

- **Risques pour la vie privée :**
  - Traçabilité illégitime des individus
  - Espionnage des activités et des informations personnelles
- **Besoins**
  - Anonymisation (identification)
  - Confidentialité des données générées par les objets (contenus)
  - Et ce avec les garanties de :
    - Scalability
    - Bon niveau de sécurité

(source : spiral-group.co.uk/)

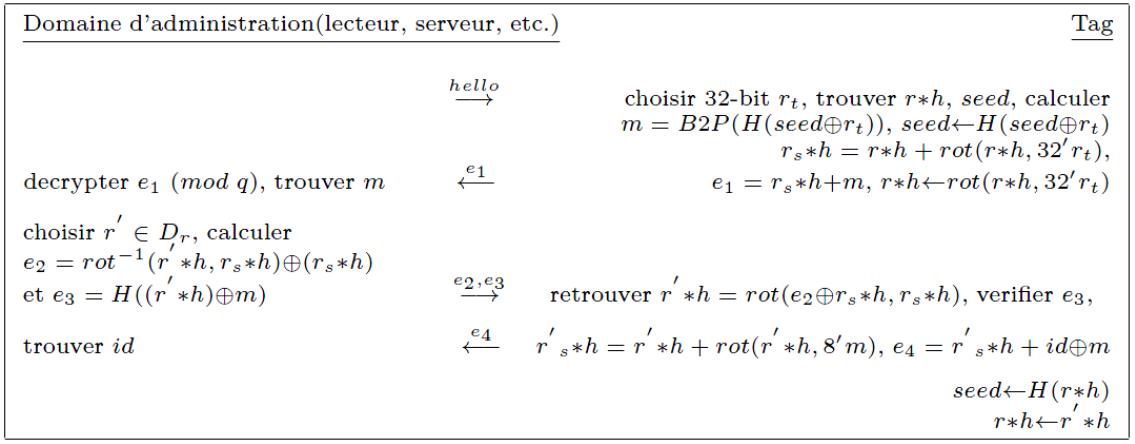
Approche de Télécom SudParis

- **Verrous technologiques :**
  - Concevoir des approches de sécurité légères visant de très faibles consommations de ressources (mémoire, calculs, batterie)

- **Résultats de l'équipe :**
  - 2 brevets sur l'authentification mutuelle légère, dont un basé sur le cryptosystème asymétrique NTRU
  - Etude de maturation (OMTE) par Digitéo en cours
  - Nomination au prix Fibre de l'innovation 2013

Brevet – « Procédé pour crypter des données dans un cryptosystème NTRU (N,p,q) »

- **Dispositif de sécurité : pour qu'un appareil de très faibles capacités (RFID, capteur…) s'authentifie et chiffre de faibles volumes de données**
- **Eléments techniques**
  - Adaptation du cryptosystème à clef publique NTRU avec répartition astucieuse de la charge de calcul
  - Propriétés : Passage à l'échelle et niveau de sécurité élevé (traçage, déni de service, rejeux)
  - Extension de l'intra-domaine à l'inter-domaine



Ces travaux prennent place au sein…

- **Chaire Institut Mines-Télécom « Valeurs et Politiques des Informations Personnelles »**
  - 1ère chaire de l'Institut Mines-Télécom
  - Chaire multidisciplinaire (juridique, technique, économique, sociale, et éthique)
  - Objectifs : aider les entreprises, les citoyens et les pouvoirs publics dans leurs réflexions sur la collecte, l'utilisation et le partage des informations personnelles, à savoir les informations concernant les individus (leurs vies privées, leurs activités professionnelles, leurs identités numériques, leurs contributions sur les réseaux sociaux, etc.) incluant celles collectées par les objets communicants qui les entourent (*smartphones*, compteurs intelligents, télévisions connectées ou jouets intelligents de type NFC, etc.)
  - http://cvpip.wp.mines-telecom.fr/

- **Action « Objets Intelligents et Internet des objets »**
  - Action du CNRS GDR ASR rassemblant industriels et académiques
  - Coanimatrices : M. Laurent (TSP) et S. Bouzefrane (CNAM)
  - Thèmes : Plate-formes de confiance, RFID, NFC, TEE, Sécurité, Protection des données personnelles, Confiance numérique, Objets communicants
  - Objectifs: regrouper la communauté française travaillant sur cette thématique, organiser des événements scientifiques, créer un club de partenaires industriels

L’équipe de recherche pluridisciplinaire

Maryline Laurent

Professeur en sciences de l’informatique

Patrick Waelbroeck

Maître de conférences en sciences économiques

Pierre-Antoine Chardel

Professeur en philosophie

Claire Levallois-Barth

Maître de conférences en droit

et les ressources STIC de l’Institut Mines-Telecom

Les cinq axes de recherche de la chaire

- Identités numériques
- Gestion des informations personnelles
- Contributions et traces
- Informations personnelles dans l'Internet des objets
- Politiques des informations personnelles

1. Régulation juridique, propriété des identifiants
2. Co-responsabilités juridique et éthique
3. Traçabilité, anonymisation
4. Gestion et sécurité des flux automatisés, dont *cloud*

Références

- **Brevets**
  - E. El Moustaine, M. Laurent, “ Procédé pour crypter des données dans un cryptosystème NTRU (N,p,q) ”, (PCT juin 2013, juin 2012).
  - E. El Moustaine, M. Laurent, “ RFID bas-coût”, numéro d’enregistrement 11 51399, février 2011.

- **Publications**
  - Y. Ben Saied, A. Olivereau, D. Zeghlache, M. Laurent, “Lightweight collaborative keying for the Internet of Things”, Elsevier Computer & security, 2014.
  - E. El Moustaine, M. Laurent, “GPS+: A Back-end Coupons Identification for Low-Cost RFID”, 6th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec’13), pages 73-78, 17-19 April 2013, Budapest, Hungary.
  - E. El Moustaine, M. Laurent, “A Lattice Based Authentication for Low-Cost RFID”, IEEE RFID Technology and Applications (IEEE RFID-TA 2012), pages 68-73, 5-7 November 2012, Nice, France.
  - Y. Ben Saied, A. Olivereau, M. Laurent, “A Distributed Approach for Secure M2M Communications”, International Conference on New Technologies, Mobility and Security NTMS 2012, May 2012, Istanbul, Turkey.