



IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom



YoGoKo

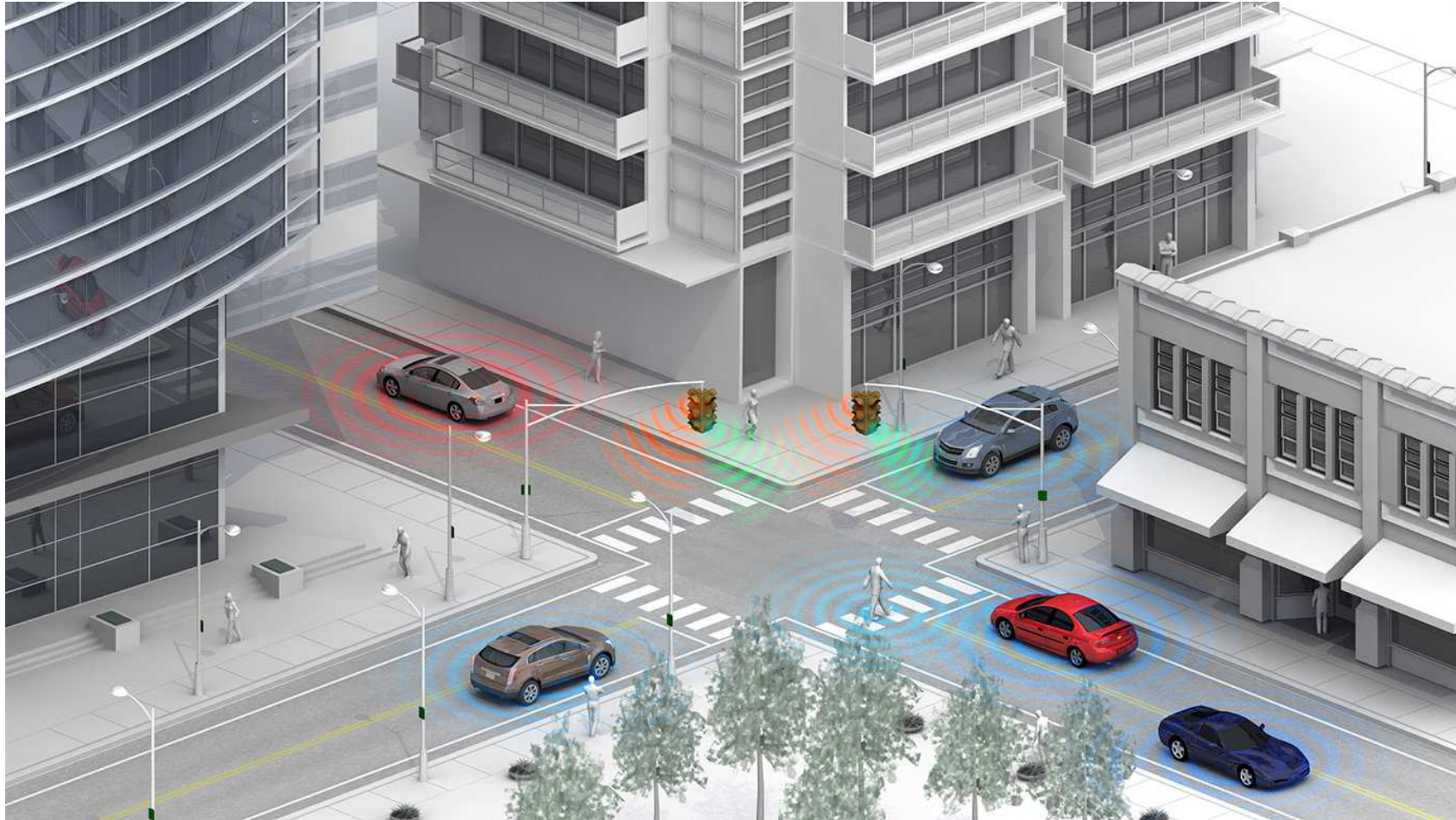
jm.bonnin@imt-atlantique.fr

SÉCURITÉ DES COMMUNICATIONS POUR LE VÉHICULE COOPÉRATIF



<https://transparencyjournal.com/iot-in-intelligent-transportation-system-market/>

C-ITS (COOPERATIVE INTELLIGENT TRANSPORT SYSTEMS)



<http://gpsworld.com/transportationroadroad-talk-11142/>

LES DÉVELOPPEMENT EN SILO CONDUISENT À ...

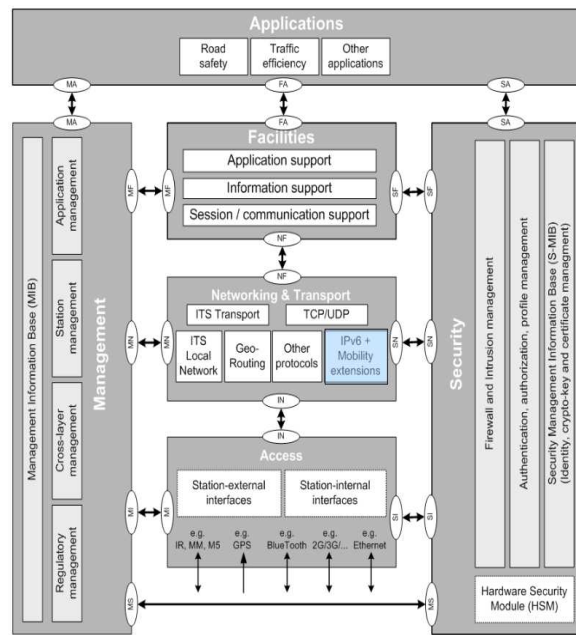




IPv6 ITS STATION STACK (ITSSv6)



ITSSv6 (IPv6 ITS Station Stack for Cooperative Systems FOTs) is a 36 months STREP starting February 2011. Its objective is to deliver an optimized IPv6 implementation of ETSI / ISO 's ITS station reference architecture. ITSSv6 starts its work from existing standards from ETSI, ISO and IETF and available IPv6 software from CVIS and GeoNet projects. Cooperative Systems FOTs and relevant European and National ICT projects will be supported in using the IPv6 ITS station stack.



ITSSv6 tasks includes:

- Gathering prospective third party users into a common User Forum to collect user's requirements
- Enhancement of existing IPv6-related ITS station standards and specification of missing features
- Implementing IPv6-related ITS station standards
- Validation of the implementation and scientifically assessment of its performance
- Porting the IPv6 ITS station stack to selected third party platform
- Supporting third parties in the use of the IPv6 ITS station stack

Coordinator: INRIA
Consortium Partners: Institut Telecom, Universidad de Murcia, SZTAKI, lesswire, IPTE, BlueTechnix

UNE ARCHITECTURES COMMUNE A ÉTÉ DÉFINIE (ISO/ETSI)

Multiple médias de communication

- M5/G5 (802.11p), IR, 2G/3G, LTE/5G, DSRC, WiFi, ...

Plusieurs modèles de communication

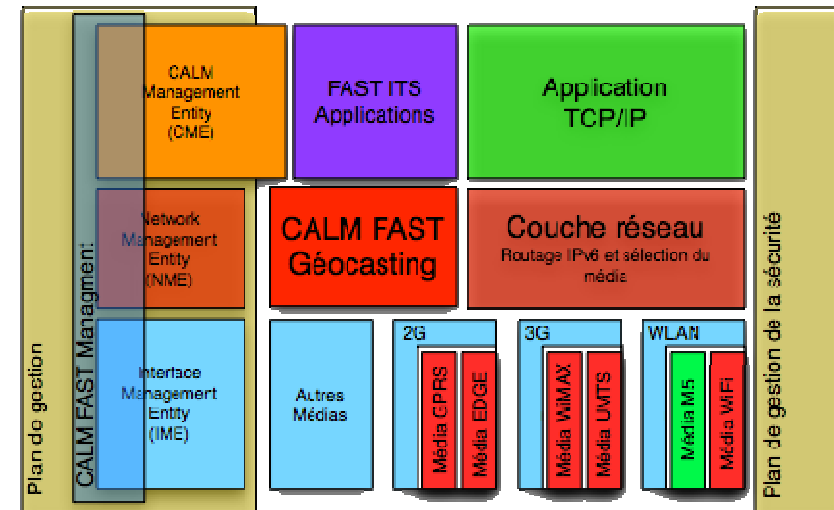
- IPv6, Mobile IPv6, network mobility (NEMO)
- V2X : à base de messages courts
 - Courte et moyenne portée, Temps-réel
 - Routage géographique
 - Une fréquence réservée

Ensemble d'outils (facilities)

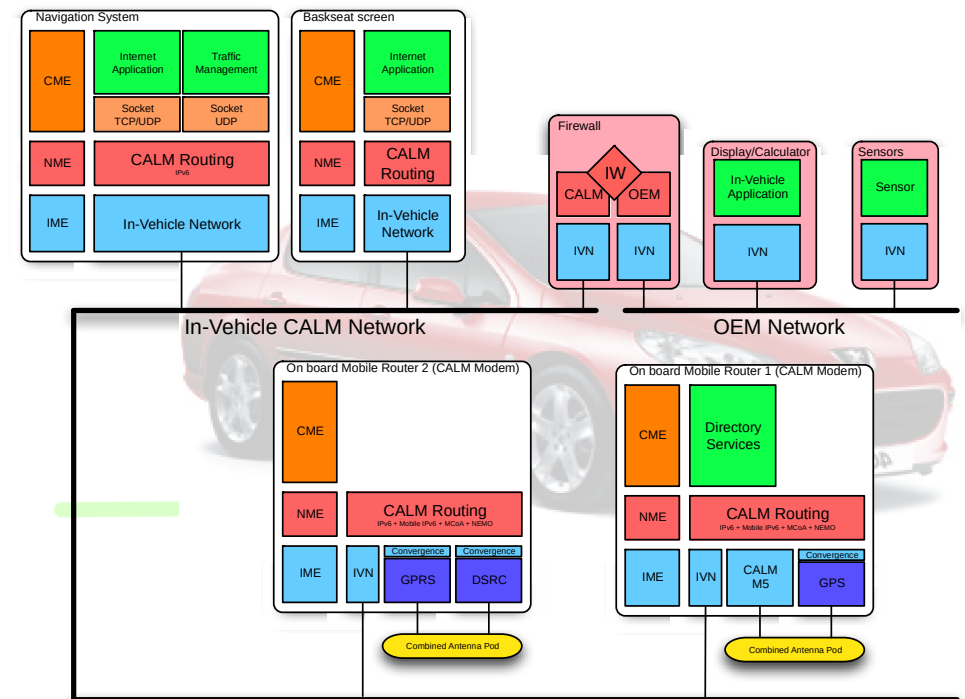
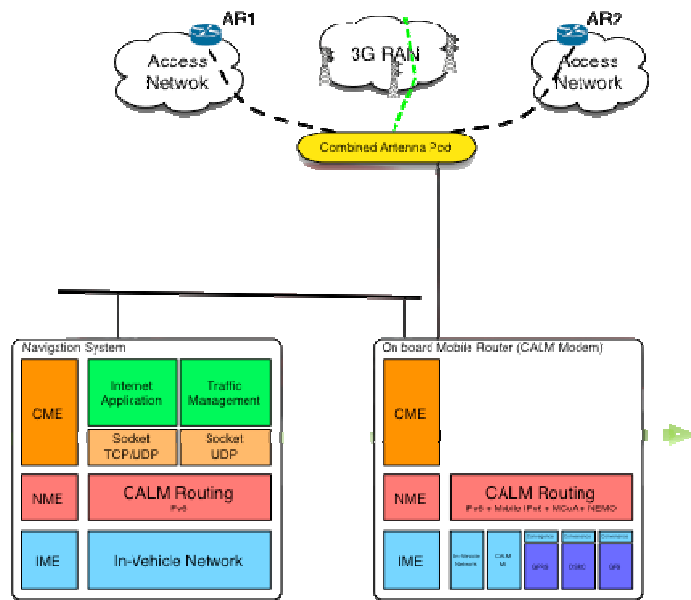
- Positionnement / Map matching,
- Capteurs
- Déploiement d'application

Un plan de management

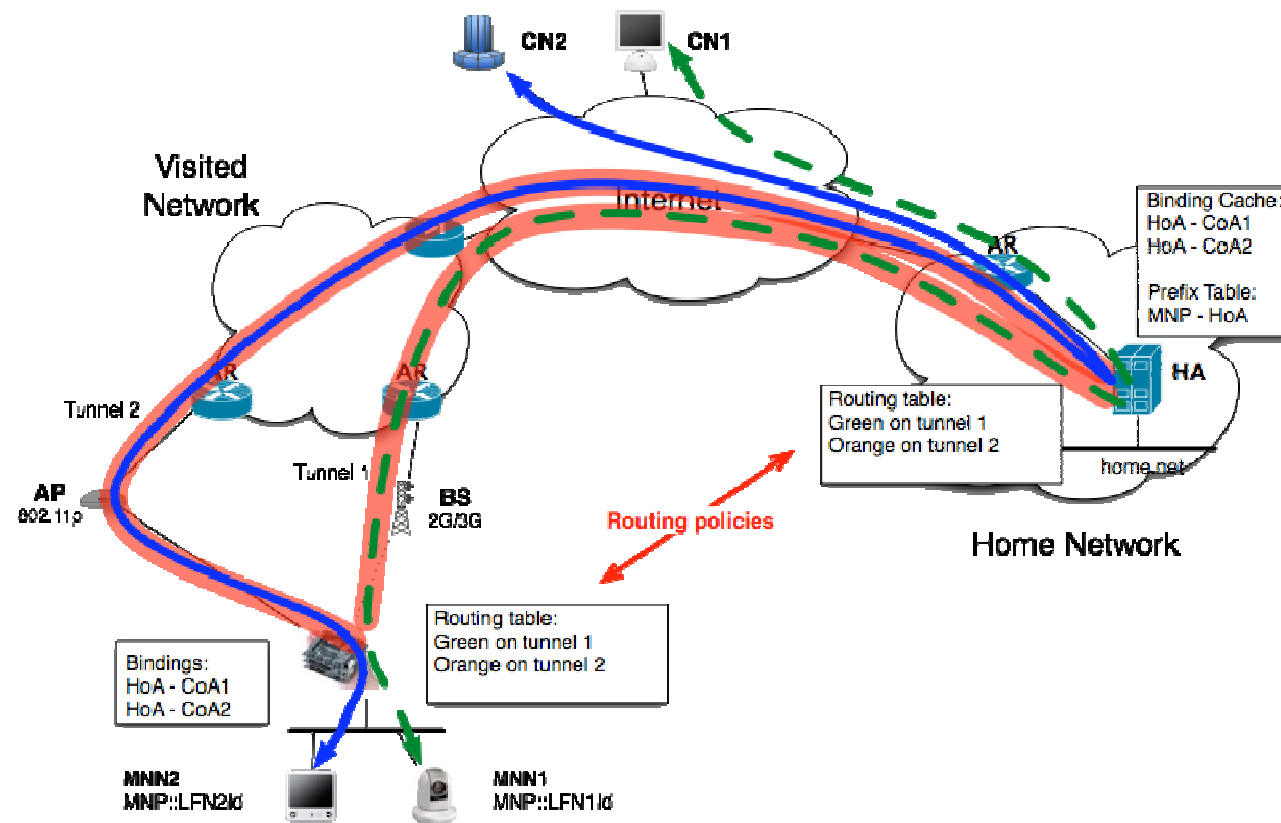
Une gestion « cross-layer » de la sécurité



UNE ARCHITECTURE FONCTIONNELLE

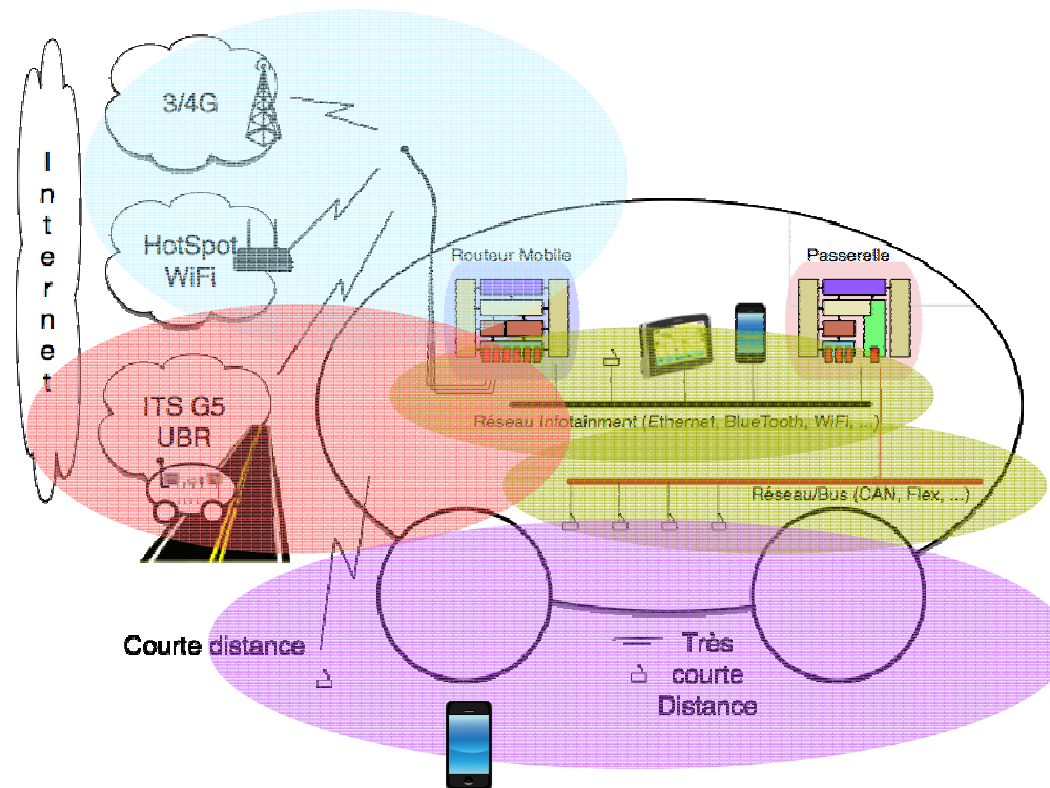


COMMUNICATIONS DE TYPE INTERNET



LA SECURITÉ

DOIT ÊTRE GÉRÉE À TOUS LES NIVEAUX DE L'ARCHITECTURE

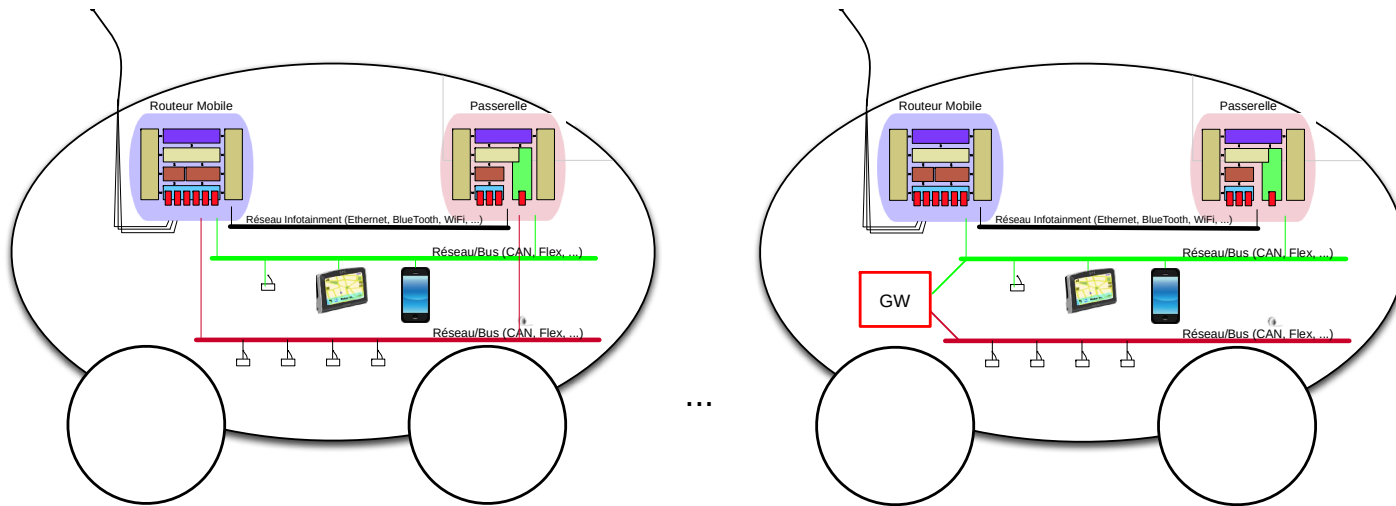


L'AUTOMATISATION CROISSANTE INDUIT DE NOUVEAUX RISQUES

La sécurité de l'informatique embarquée devient extrêmement critique

Le logiciel contrôle tout dans le véhicule

=> Une architecture redessinée pour isoler les fonctions critiques



Mais ce n'est pas suffisant ...

LES BESOINS EN TERME DE SÉCURITÉ

Besoins élémentaires

Authentication

Intégrité

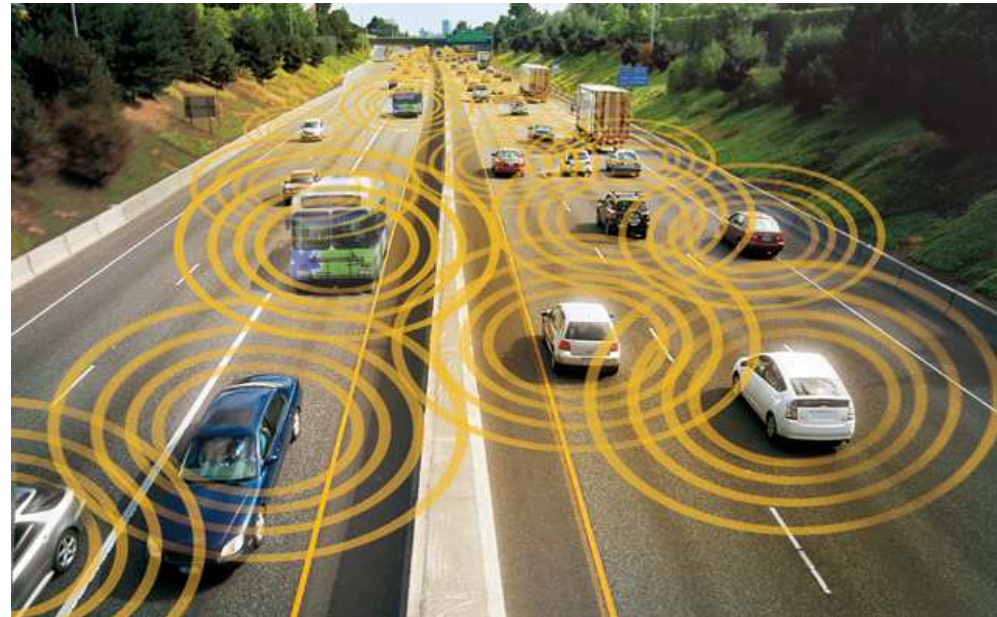
Anti-rejeu

Seulement si nécessaire

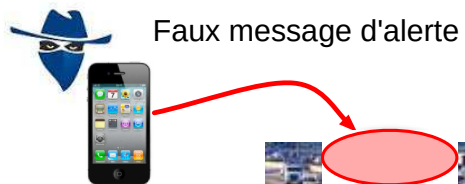
Non-répudiation

Toujours requis

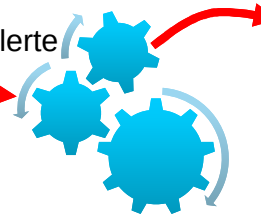
Respect de la vie privée



POURQUOI LA SÉCURITÉ EST-ELLE SI CRITIQUE ?



Vrai message d'alerte



Avant de prendre en compte un message

- Qui a envoyé le message ?
- Était-il légitime pour le faire ?
- Le message a-t-il été modifié ?
 - Date
 - Position
 - Contenu

Contraintes pesant sur le mécanisme de sécurité :

- Délai (Real time)
- Capacité de calcul (nombre de messages par seconde)
- Surcharge protocolaire
- Respect de la vie privée

MÉCANISMES DE SÉCURITÉ

Algorithme de cryptographie

Clés asymétrique vs. clé symétrique

Approche à base de clé symétrique (partagée)

La clé est un secret partagé.

Ex: 3DES

Approche à base de clé asymétrique

Deux clés par entité (publique, privée)

Ex: RSA, ECDSA (public key cryptography system)

RESPECT DE LA VIE PRIVÉE vs. SÉCURITÉ

Respect de la vie privée (Privacy)

La position de l'utilisateur est une donnée sensible

i.e. toute relation entre des données et un localisateur doit être protégée

Beaucoup d'applications ont besoin de la position

⇒ **Ne pas dévoiler des éléments d'identité lorsqu'on échange une position.**

⇒ **i.e. cela inclut toute information pouvant conduire à inférer une identité**

Adresses, certificats, informations trop spécifiques, ...

Mais l'identité est nécessaire pour la sécurité

Non-répudiabilité (Accountability)

⇒ Notion de pseudonymes

PSEUDONYMES

Un identifiant anonyme !

- Choisi aléatoirement**

- Permet de remplacer un identifiant (Adresse IPv6 ou MAC, ...)**

- Doit être unique dans son domaine d'usage**

Notion de certificat pseudonyme

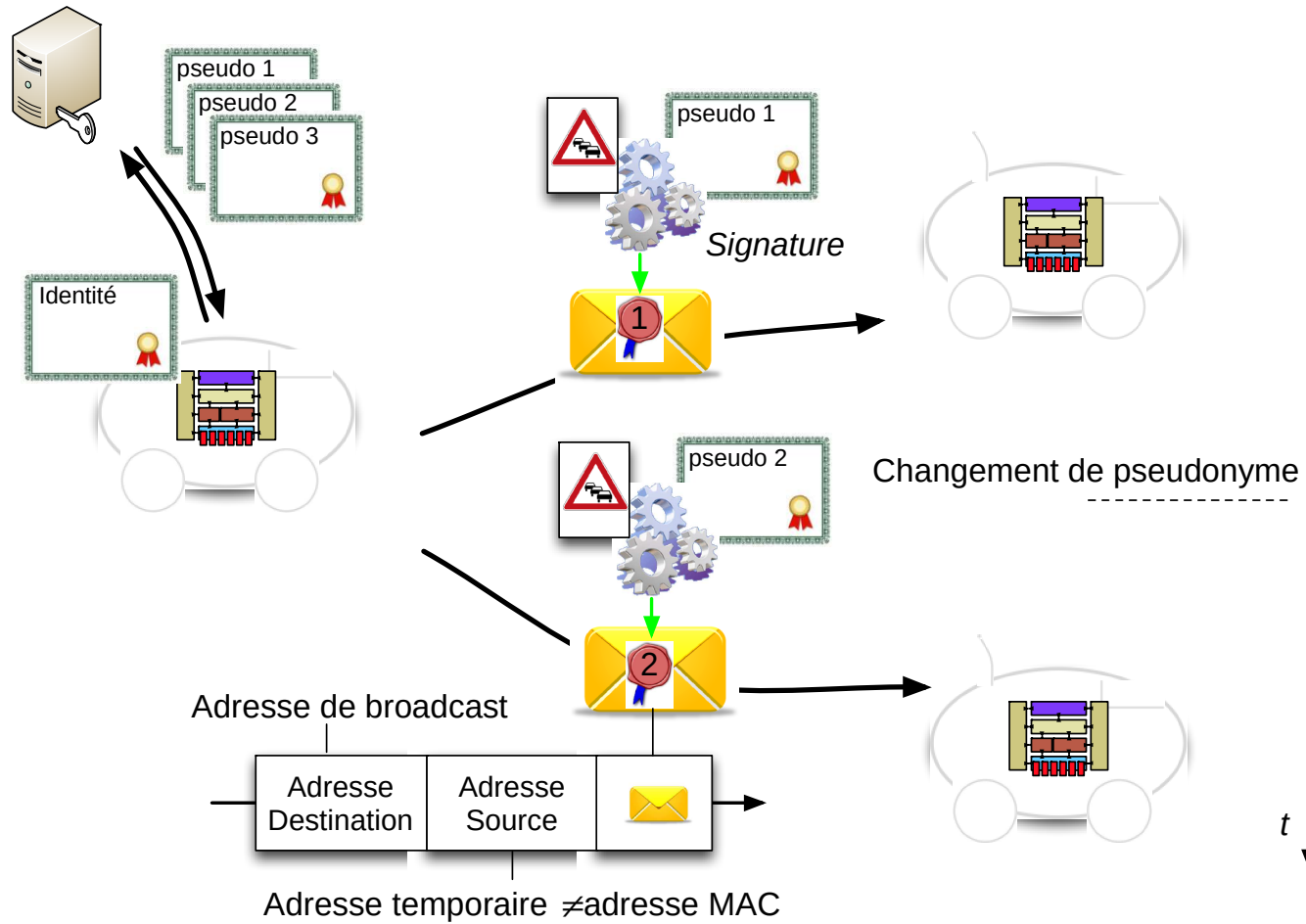
- Valide pour une durée limitée**

- Etablit par une autorité de certification**

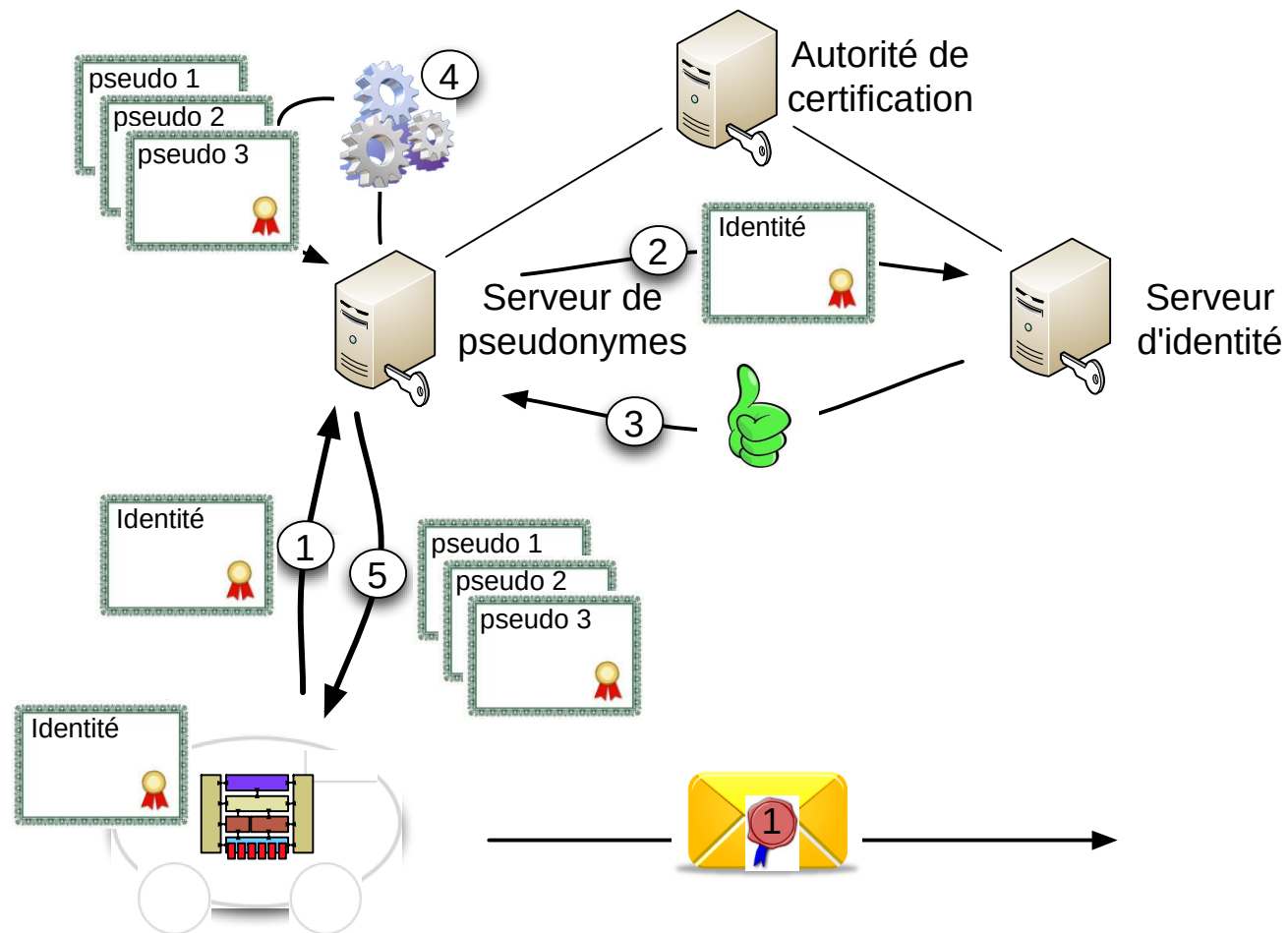
- Permet à l'autorité de remonter au certificat long-terme**

- Seule l'autorité légitime peut lier les certificats**

CERTIFICATS PSEUDONYMES



GESTION DES CERTIFICATS



AVANTAGES DES PSEUDONYMES

Permet d'éviter des attaques potentielles

Sans empêcher les applications légitimes de fonctionner

Assure le respect de la vie privée (limité)

Le mécanisme des certificats pseudonymes

Permet de signer les messages avec une identité temporaire

Seule l'autorité légitime peut retrouver l'identité permanente

Tous les identifiants ou pseudo-identifiants doivent être cachés

Utilisation de pseudonyme (identifiant aléatoire)

Dans toutes les couches de communication

... Inconvénients :

Parfois difficile d'éviter de donner des indices

Qui permettent à un observateur de lier deux pseudonymes consécutifs.

Lourd et difficile à mettre en œuvre

CONCLUSION & PERSPECTIVES : SMART-CITIES

L'environnement dans les villes « intelligentes » :

- **Sera Hétérogènes**

- Technologies de communications, services, équipements connectés, ...

- **Evoluera rapidement**

- Déploiement incrémental

- **Devra gérer un très grand nombre d'équipements**

- Une très grande quantité d'information

- Inabordable dans une mutualisation de l'infrastructure



- Relocaliser les interactions peut être une partie de la solution :

Comment communiquer avec des correspondants non connus ?

Comment faire confiance aux données qu'ils nous envoient ?

**QUESTIONS
/
COMMENTAIRES**





Testing & learning about
**DIGITAL MOBILITY
SOLUTIONS**^{3,1}
in RENNES
14th > March 2019
2019 < March 2018
www.inout2019.com



Écosystème mobilité

Industrie des
télécommunications

Intégrateurs de systèmes

ENTREPRISES INNOVANTES

SENIORS

ETUDIANTS

START-UPS

Fournisseurs de service

Application mobile

CONSULTANTS

Opérateurs de réseau mobile

Jeunes

INDUSTRIE AUTOMOBILE



INVESTISSEURS

Assureurs

USAGERS

Institutionnels

Chercheurs

Nouvelle économie

Infrastructure

SMART CITIES

Agences gouvernementales

Economie traditionnelle

DÉVELOPPEURS

Associations de consommateurs

Écosystème numérique