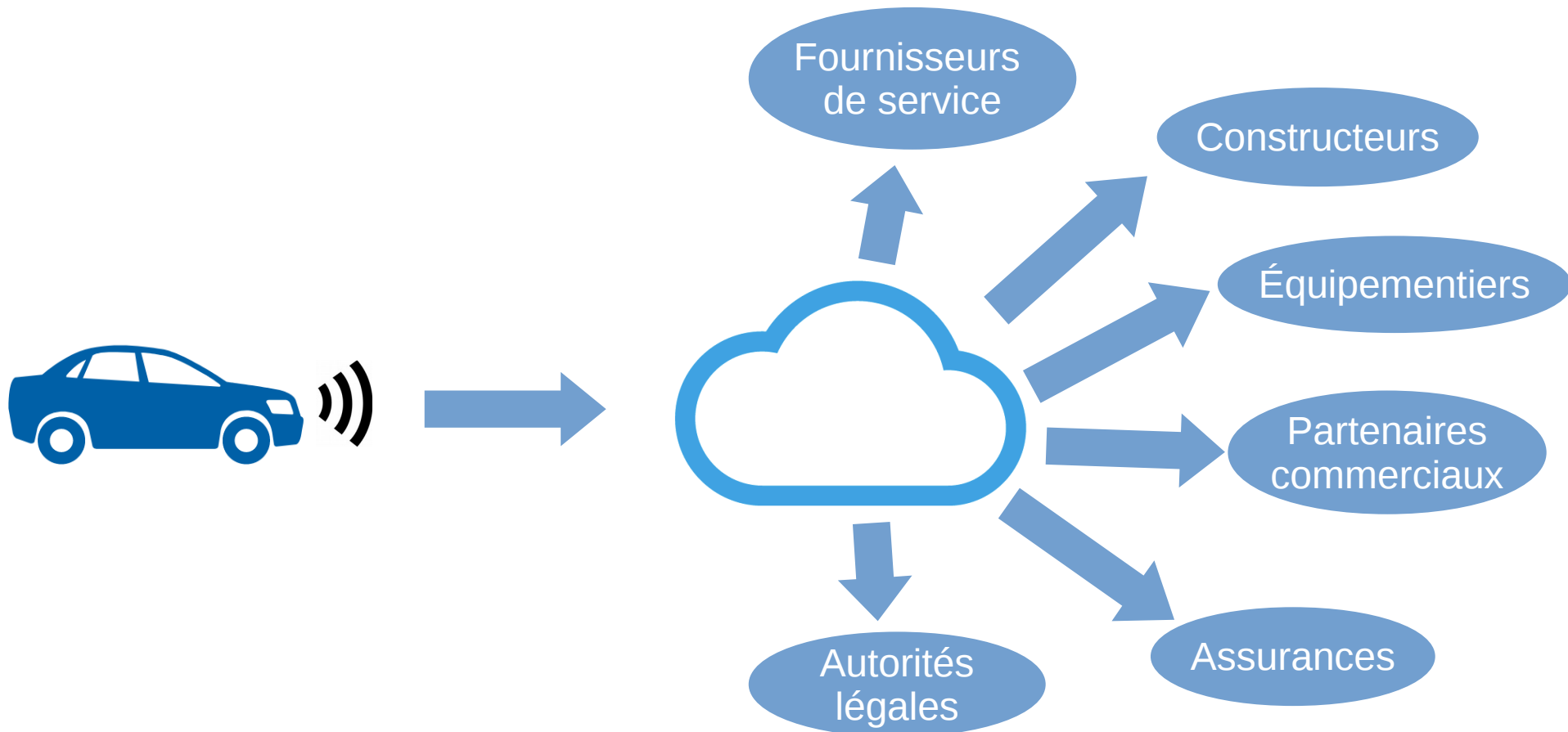


Une politique de contrôle d'accès aux données pour les systèmes de transport intelligents

Rémi Adelin

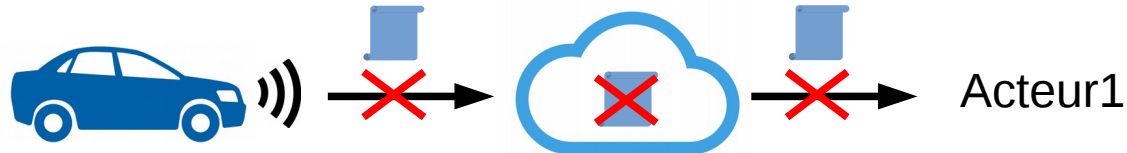
Vincent Nicomette Eric Alata Vincent Migliore Mohammed Kaâniche
TSF, LAAS-CNRS, Toulouse, France

Perte du contrôle des données par les conducteurs

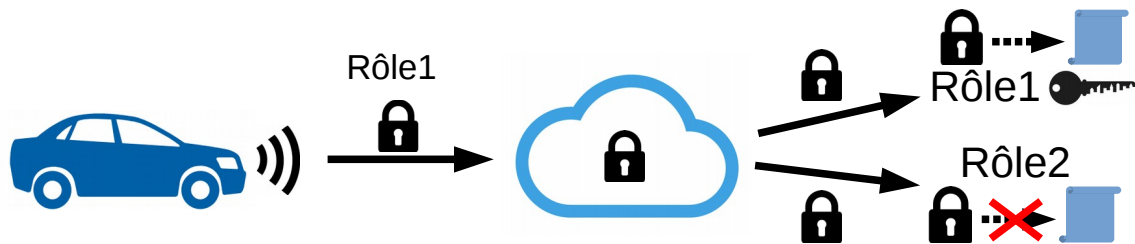


Politique de contrôle d'accès

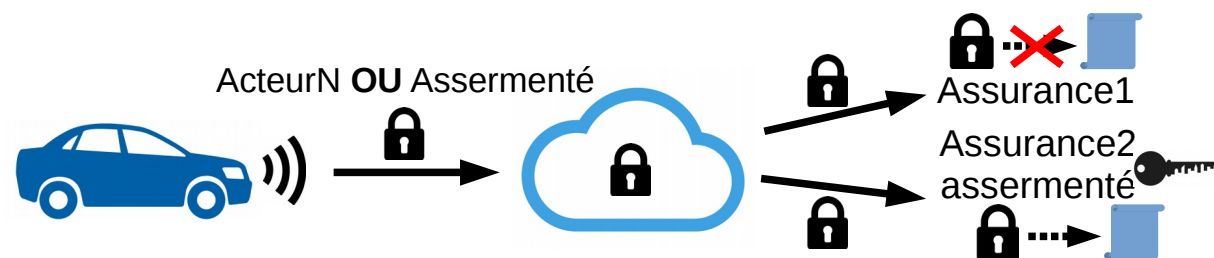
1) Interdire le stockage en clair



2) Le conducteur définit le contrôle d'accès

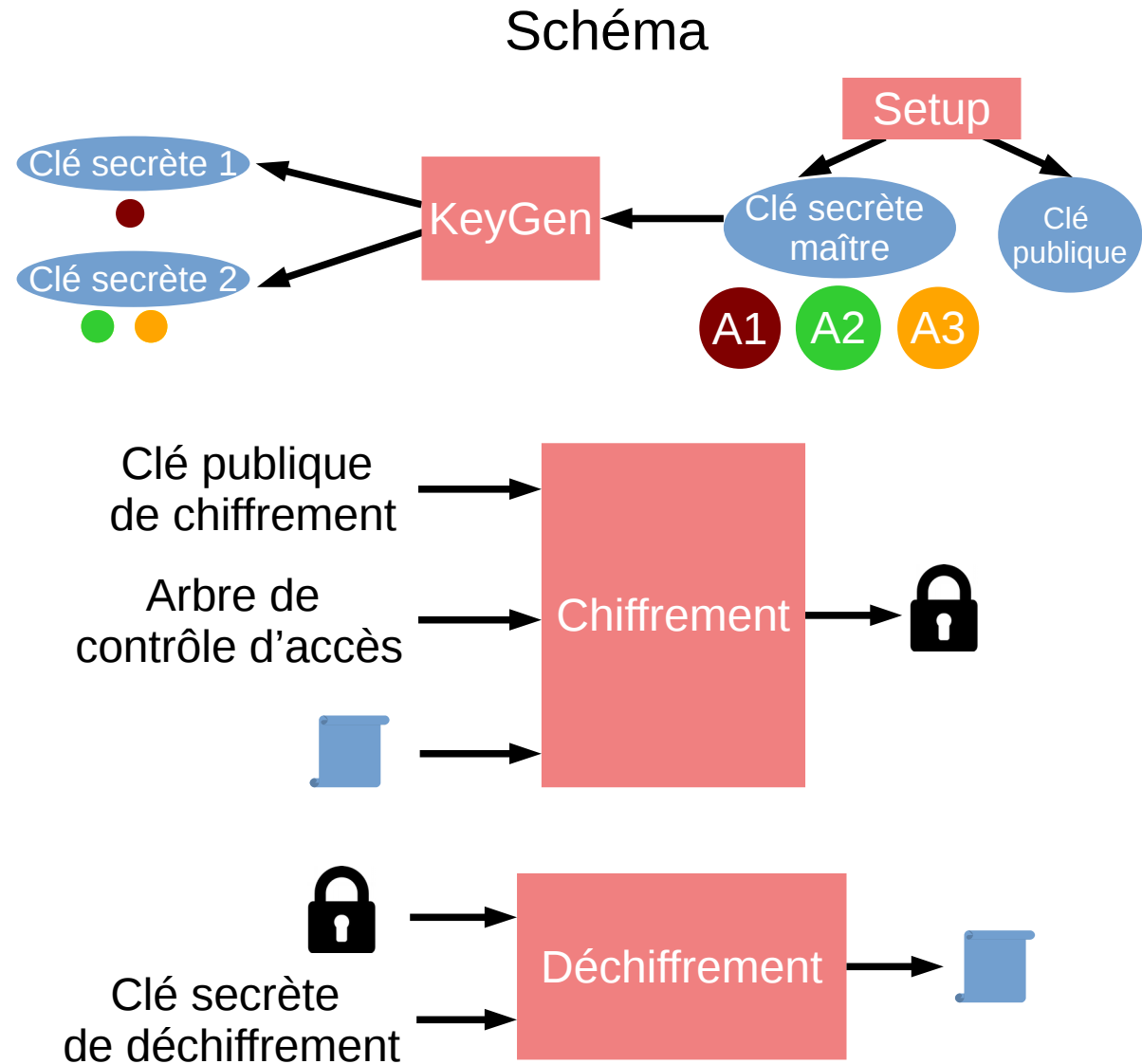
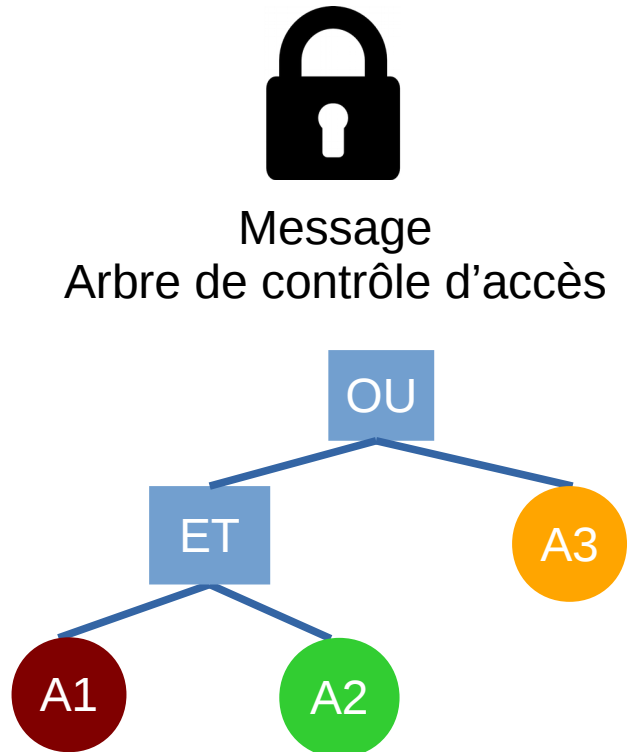


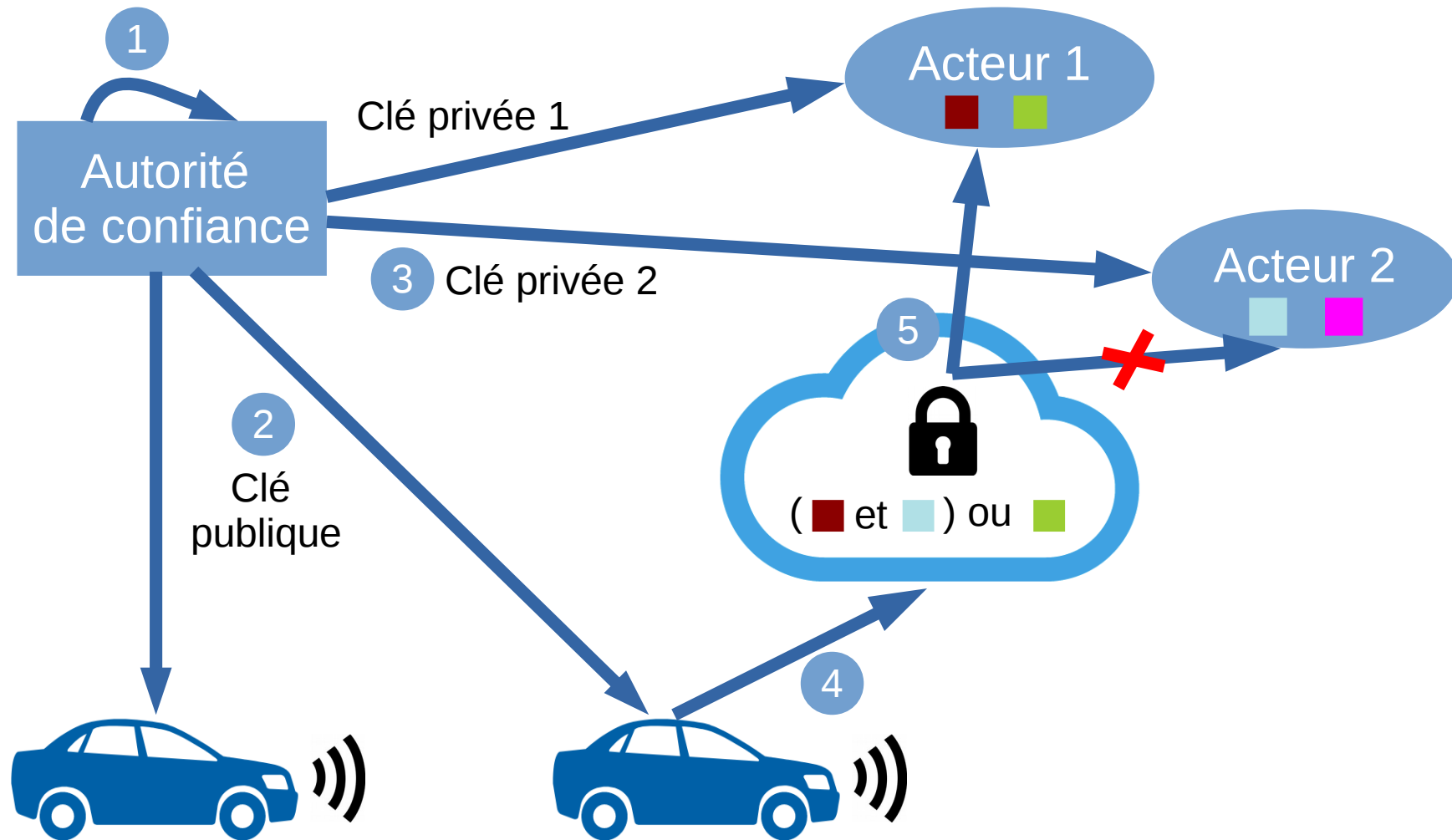
3) Exceptionnellement outrepasser les droits



Chiffrement par attributs

CP-ABE (Ciphertext-Policy Attribute-Based Encryption)
(John Bethencourt, Amit Sahai, Brent Waters, 2007)



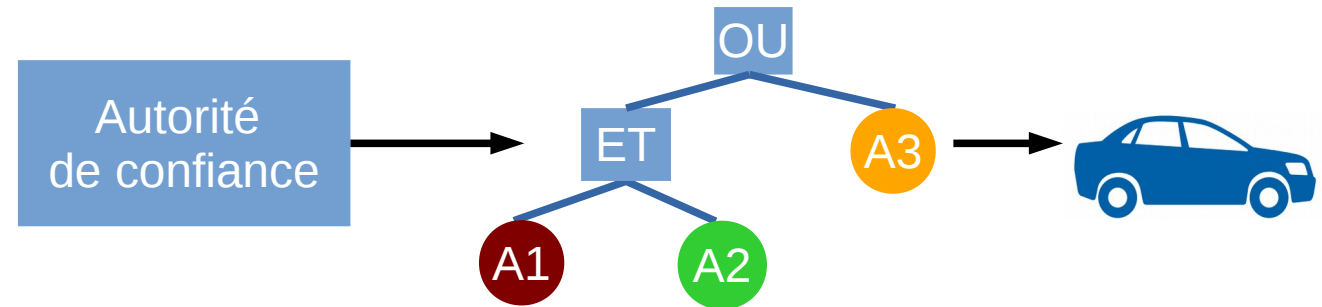


Mise en place des attributs

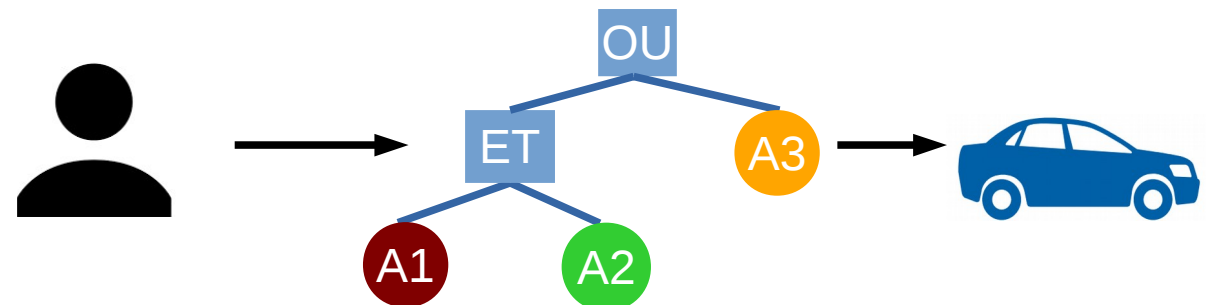
Attributs

- Caractérisation des acteurs
 - Rôle
 - Restriction géographique
 - Assermenté
 - ...
- Caractérisation des données
 - Niveau de criticité
 - Origine de la donnée
 - ...

Arbre de contrôle d'accès



Pré-provision des arbres obligatoires



Définition des arbres par l'utilisateur

- Révocation
- Authentification
- Contrôle d'intégrité
- Confiance dans la donnée
- Descente d'information
- ABE post-quantique
- Efficacité de la solution
- Espace des attributs