

La sécurité

Houda Labiod – Télécom Paris

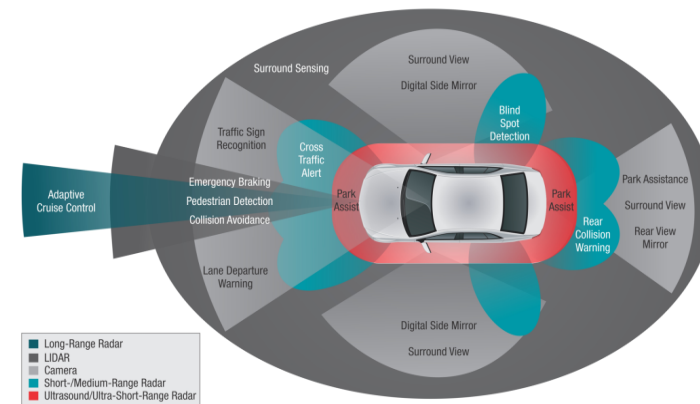
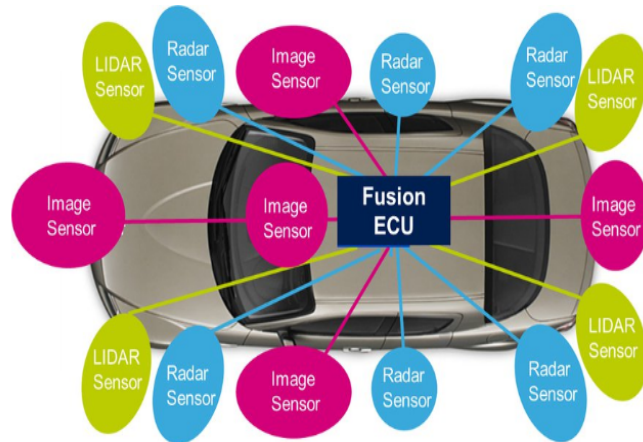
houda.labiod@telecom-paris.fr

Workshop C-ITS France, Institut des Mobilités et des
Transports Durables

13 Mars 2020, Valenciennes

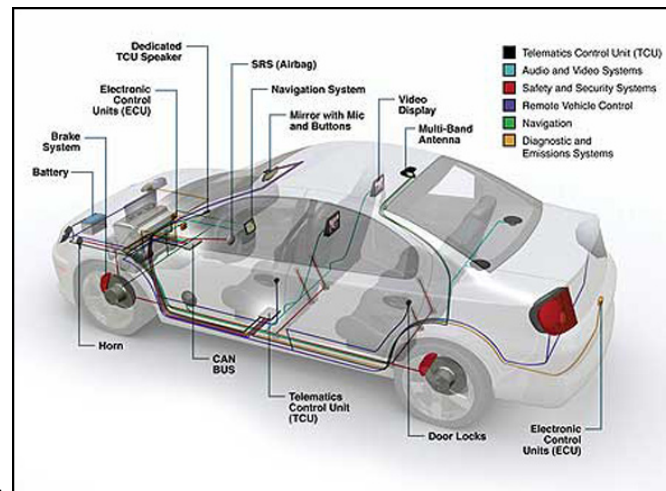


Co-financed by the European Union
Connecting Europe Facility



2000 capteurs dans un
véhicule connecté

Perception



Communication
(ECU, bus CAN, OBU,...)

La connectivité augmente les surfaces d'attaque

- Plusieurs surfaces d'attaque évolutives
 - Les points de communication du véhicule et de l'extérieur
 - La connectivité entre réseaux (CAN / extérieur, ...)
 - Le logiciel embarqué et débarqué
 - Les protocoles de communication
 - Le système d'authentification (usurpation d'identité)
- Les services augmentent les surfaces d'attaque
- La cybersécurité concerne un écosystème complet impliquant une interopérabilité interentreprises, inter-acteurs,et donc inter-systèmes
- Approche cross-layer



<https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>.

Risques :
malveillance, vol,
activation d'options
payantes,
atteinte à la vie
privée...

Sécurité dans InterCor

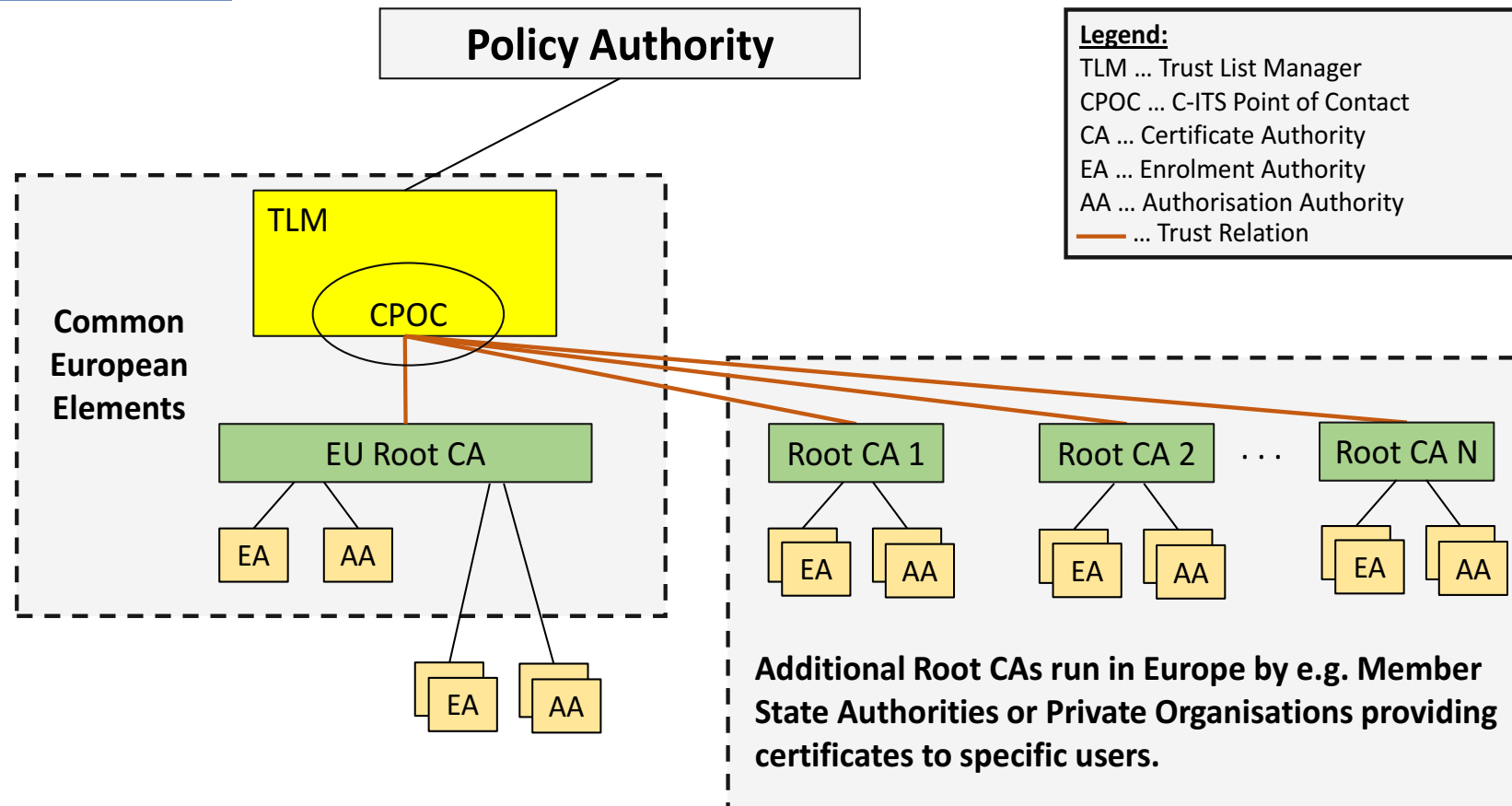
Principaux objectifs

- Spécification du système de confiance (PKI)
- Interopérabilité inter-PKIs
- Sécurisation des communications hybrides
- Conformité aux standards de sécurité ETSI



- Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)
- Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)

Modèle de confiance Européen



Modèle de confiance basé sur une chaîne de certification hiérarchique

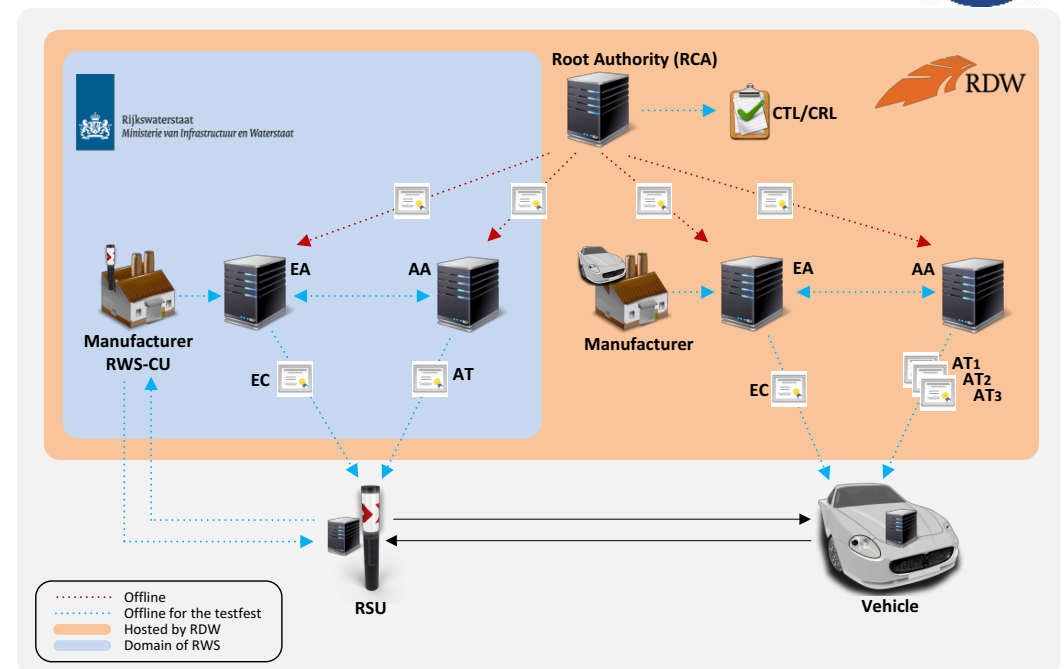
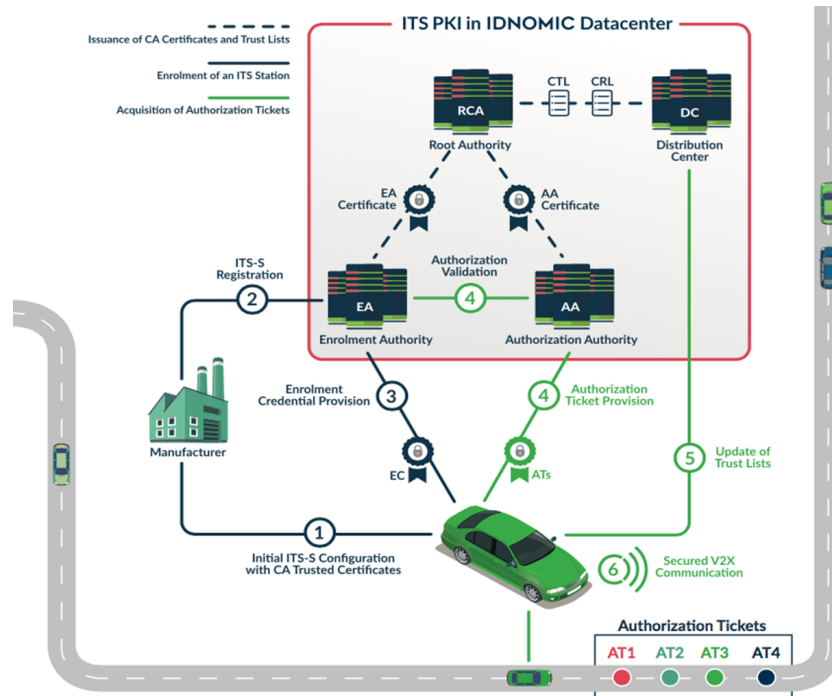


Co-financed by the European Union
Connecting Europe Facility

Source: European Commission
Certificate Policy, Release 1, Juillet 2017



InterCor 4 PKIs



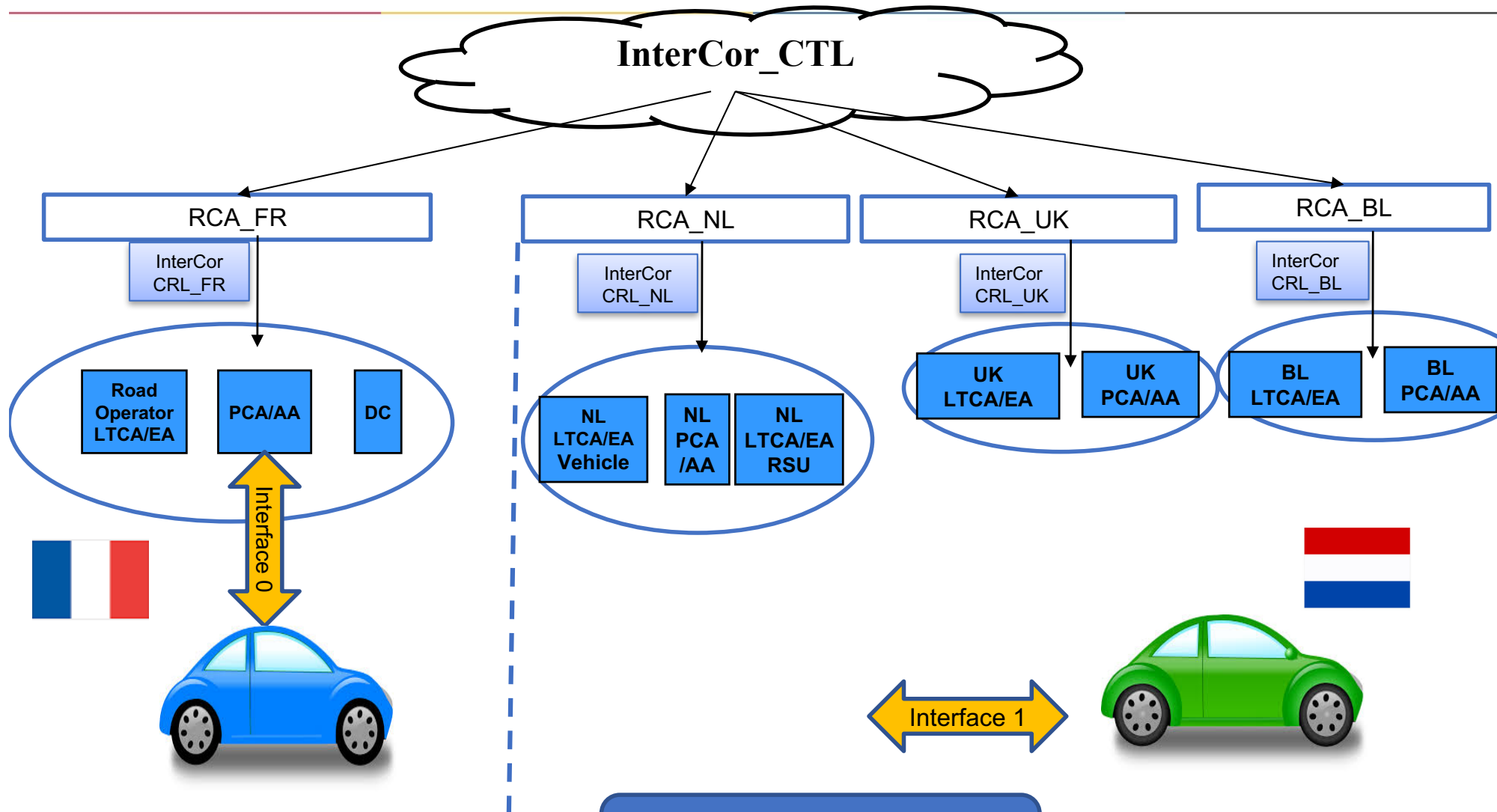
Les partenaires InterCor ont implémenté un modèle de confiance global simplifié conforme à celui défini par la CE.
Standards de sécurité: ETSI 103097 version 1.2.1 et ETSI TS 102941 v1.1.1.
Pour les structures CTL et CRL, les formats définis dans le projet SCOOP@F ont été utilisés.



Co-financed by the European Union
Connecting Europe Facility

Pas de PA, pas de TLM,
et pas de CPOC

InterCor Modèle de confiance global



Co-financed by the European Union
Connecting Europe Facility

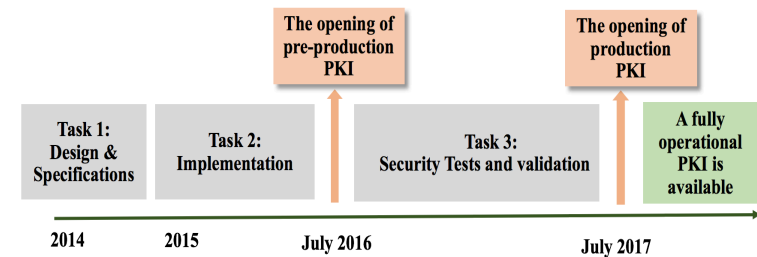
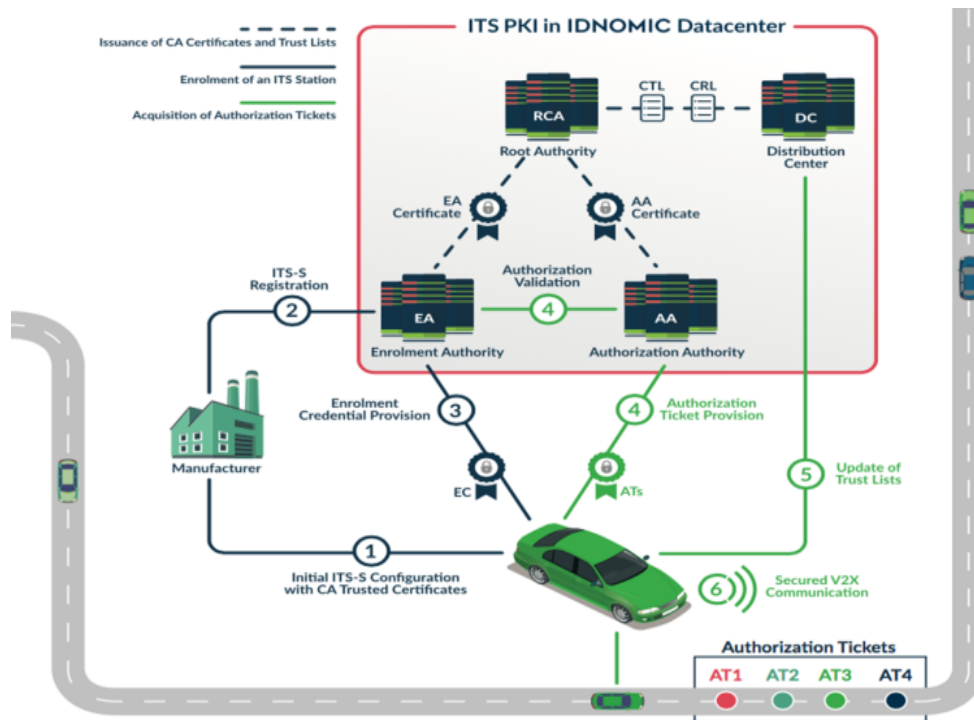
InterCor_CRL commune &
InterCor-CTL commune



MINISTÈRE
DE LA TRANSITION
ÉCOLOGIQUE
ET SOLIDAIRE

MINISTÈRE
CHARGÉ DES
TRANSPORTS

InferCor Notre PKI française



Cérémonie des clés

Une solution de sécurité pleinement opérationnelle

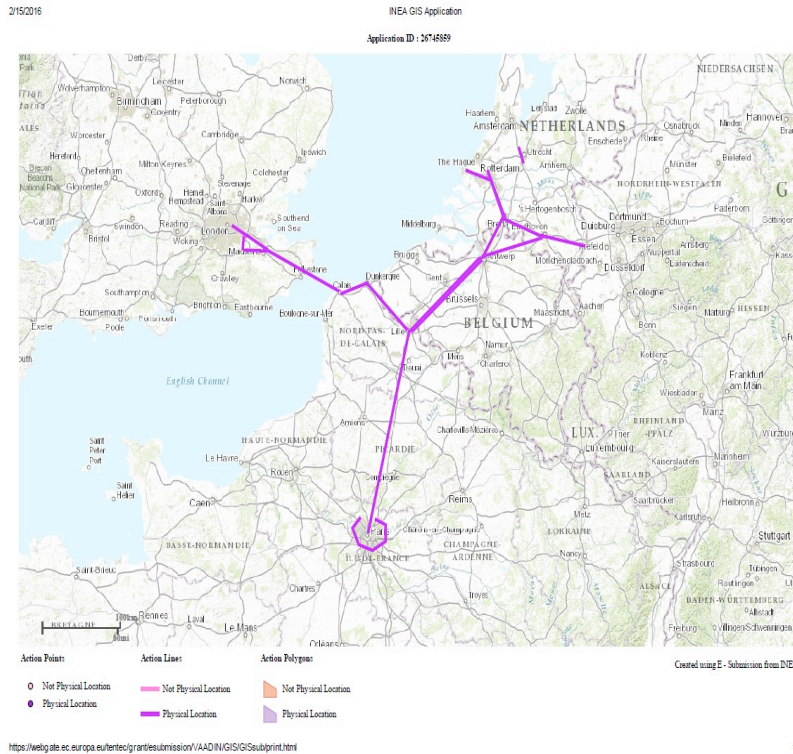
- ✓ Conçue et mis en œuvre
- ✓ Conforme aux standards ETSI (TS 103 097 v1.2.1, TS 102 941 v1.1.1,...)



Co-financed by the European Union
Connecting Europe Facility

InferCor Tests croisés & Interopérabilité

144 participants, 27 institutions - 11 pays
10 PKIs, 12 RSUs, 22 OBUs



TESTFEST#2 PKI-Security, Reims, Avril 2018

Premier évènement de test de grande envergure à l'échelle Européenne



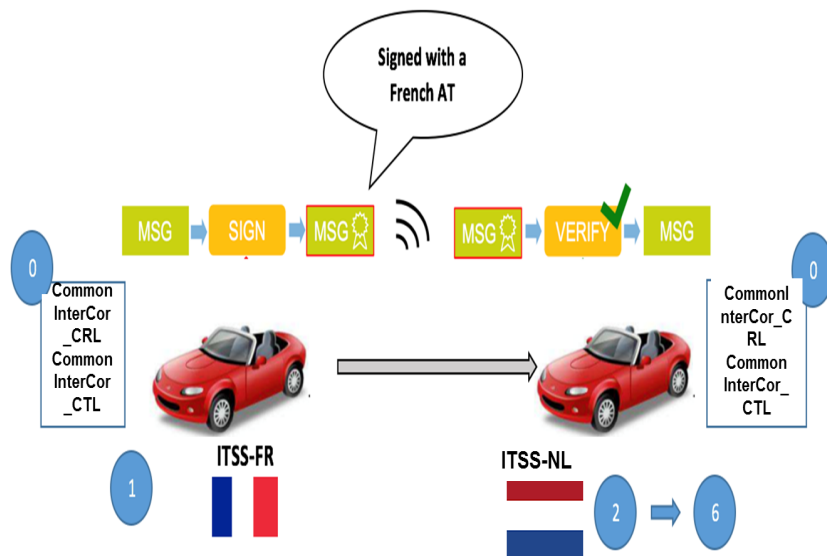
Un grand succès



Co-financed by the European Union
Connecting Europe Facility

Tests de sécurité

Tester l'interopérabilité entre 4 PKIs



Messages signés avec des certificats PC/AT pré-téléchargés, CTL commune et CRL commune pré-téléchargées

Test ID	Description
Security TESTFEST_1	Verification of message signature received from a foreign ITSS and signed with a valid AT.
Security TESTFEST_2	Verification of message signature received from a foreign ITSS and signed with an AT issued by a revoked foreign AA.
Security TESTFEST_3	Verification of message signature received from a foreign ITSS and signed with a valid AT but the common InterCor_CRL has expired
Security TESTFEST_4	Verification of message signature received from a foreign ITSS and signed with an AT issued by a non-trusted foreign RCA.
Security TESTFEST_5	Verification of message signature received from a foreign ITSS and signed with a valid AT with a new updated InterCor_CTL

TS 103097 v1.2.1, TS 102941 v1.1.1
Formats de SCOOP@F pour les CTL/CRL

Vérification de la validité de la chaîne de confiance
 Vérification de la signature des messages C-ITS



Co-financed by the European Union
 Connecting Europe Facility

Vers la migration ...

PoC de test du standard de sécurité TS 103097 v1.3.1

Collaboration Télécom Paris-NeoGLS

Matériel



RSU



OBU1



OBU2



Ordinateur 1



Ordinateur 2



La Chaire C3S

« Connected Cars & Cyber Security »

**CHAIRE
CONNECTED CARS
& CYBER SECURITY**



Co-financed by the European Union
Connecting Europe Facility

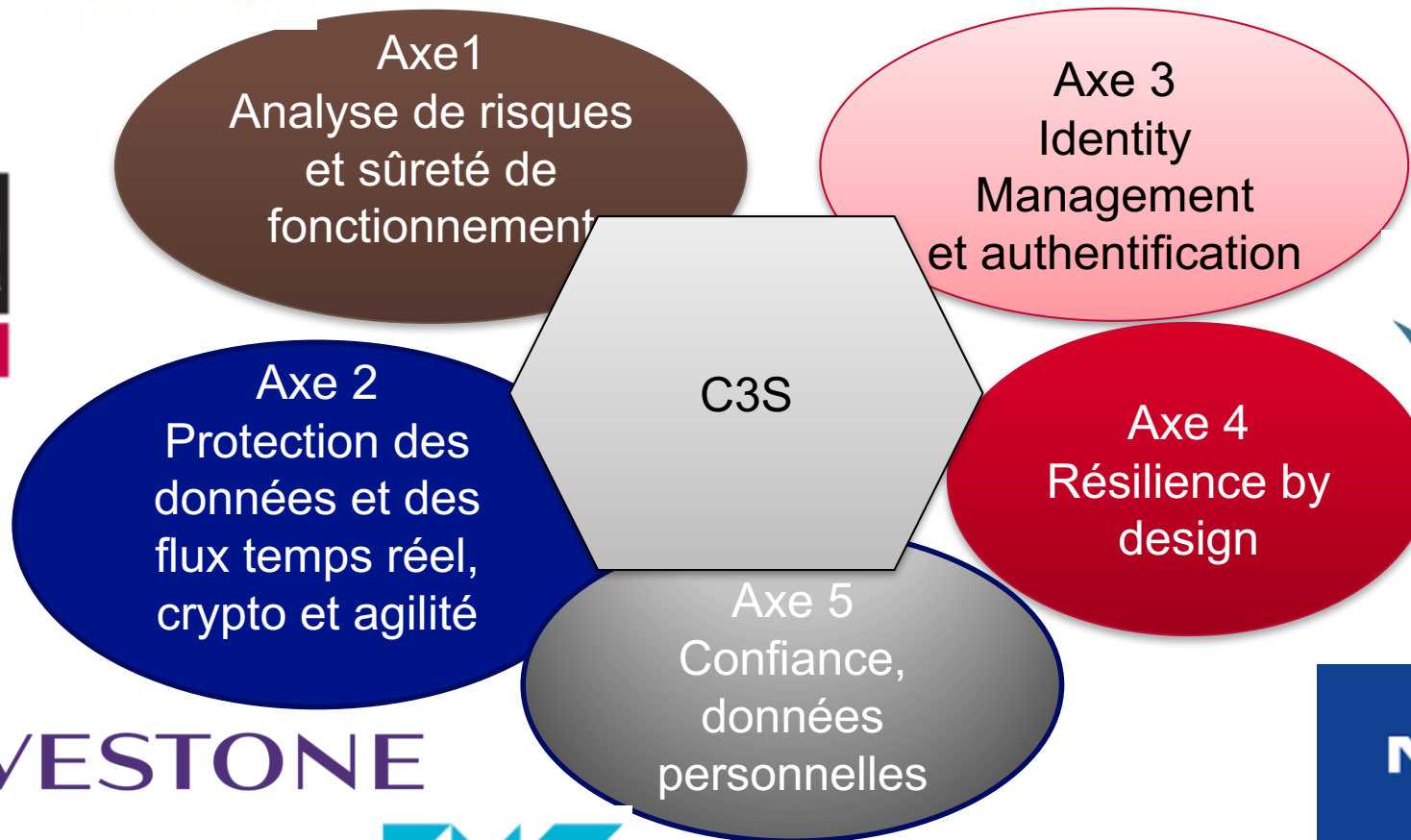
- **Chaire inaugurée en octobre 2017, durée = 5 ans**
- **Partenaires : Renault, Nokia, Télécom ParisTech, Thalès, Valeo, Wavestone, Fondation Mines-Télécom**
- **Participants: ANSSI, Délégation à la sécurité routière**
- **Porteurs : Guillaume Duc / Houda Labiod**
- **Equipe pluridisciplinaire**
 - 3 Départements : INFRES, COMELEC, SES
 - 18 enseignants-chercheurs impliqués
- **Une dizaine de doctorants et plusieurs post-doctorants**



THALES



WAVESTONE



Co-financed by the European union
Connecting Europe Facility

<https://chairec3s.wp.imt.fr/>

Merci pour votre attention.



Contact

Houda Labiod

Equipe CCN - Département INFRES-
Télécom Paris

Email: houda.labiod@telecom-paris.fr



Co-financed by the European Union
Connecting Europe Facility

info@InterCor-alliance.eu