1. SCOOP@F project

The SCOOP@F project focuses on road safety and traffic management services, based on CAM emission (10/s) and automatic emission of DENMs according to the C2C-CC triggering conditions.

SCOOP@F aims at deploying 3000 vehicles and covering2000 km of roads, including different types of road on 5 pilot sites. It has planned cross-tests with Austria, Portugal and Spain.

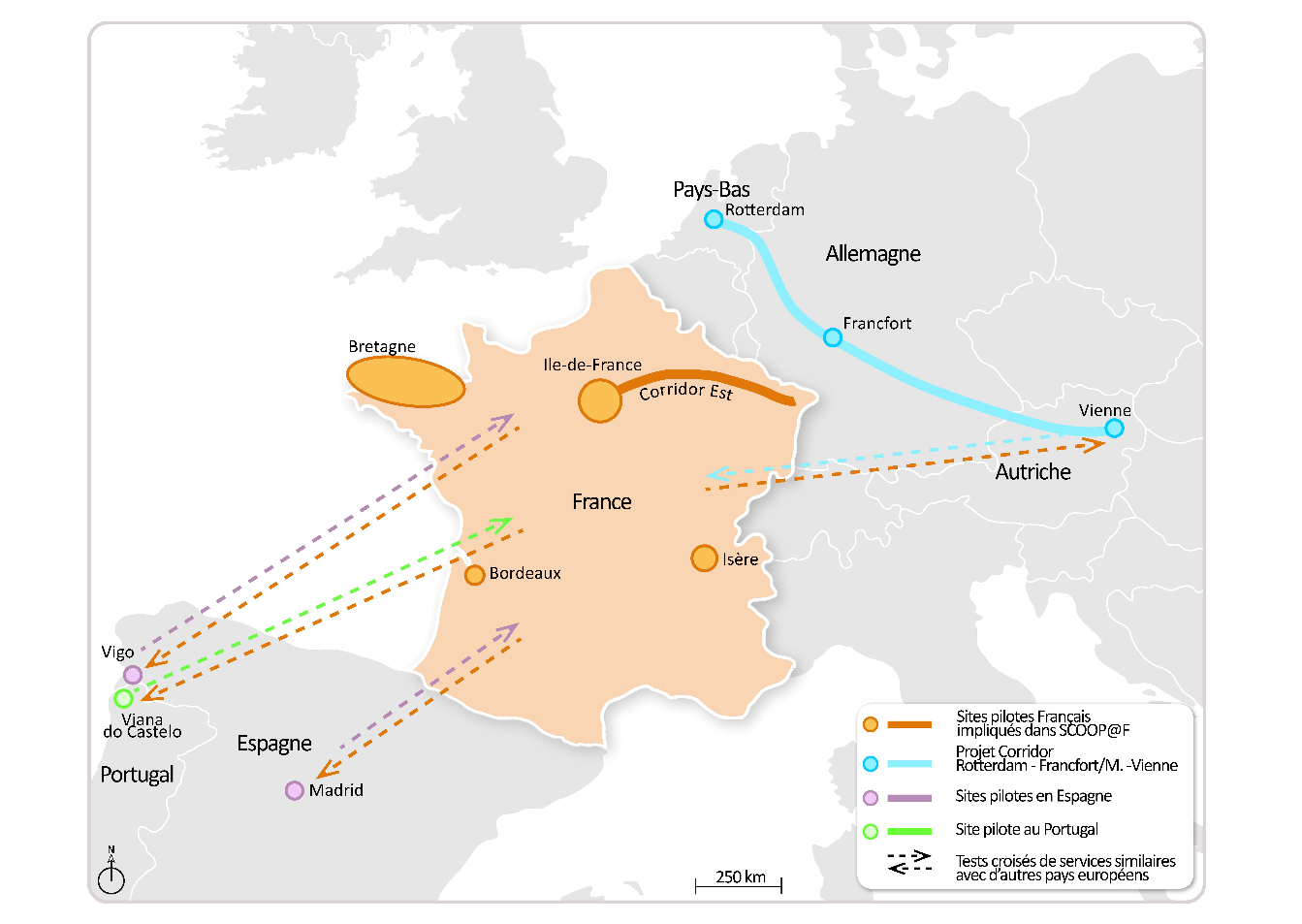


Figure 1: Overview of Scoop@F project

SCOOP tackles the following aspects in real life:

* Security: a fully operational PKI, work with ANSSI
* Privacy: included in the design of the system, work with CNIL (vehicles really sold to customers)
* Procurement: all road operators have gone through standard procurement processes, common procurement also tested
* Industrial process: the car manufacturers have worked with their usual suppliers and included the solution in their navigation system, according to industrial process and human factors considerations (ergonomists involved in the development of the HMI)
* Compliance assessment: a thorough validation process resulting in „stamps“ from the project has been defined

A cost and performance driven technical solution

Different kinds of services have to be considered:

* Services such as “urgent brake” or “End of queue” are time-critical use cases. They need to be supported by G5/DSRC technology since LTE/3G/4G:
  + Presents too much latency,
  + Doesn’t cover 100% territories in Europe,
  + Supposes a complementary investment for dynamic Device-to-Device communication, i.e. high speed broadcast.
* Non-time-critical services could be supported by G5/SDRC or LTE/3G/4G. However, the choice for SCOOP@F was all about country LTE coverage and costs considerations. Considering that LTE needs a complementary investment for broadcasting, that one G5 road side unit only costs 10k€, SCOOP@F has chosen G5 as the basic technology for all communications.

5G technology not being completely specified, this option has not been considered for any case.

Since cellular solutions suppose high costs in using them, since G5 is free access, TELCO-based solutions have not been considered as the basics.

Of course, security and privacy costs due to the PKI solution should be taken into account. But, for now, WG5 and WG6 haven’t given enough visibility on the technical scenarios considered.

However, it will take some time to deploy road side units. SCOOP@F has considered a hybrid solution based on LTE for vertical/hierarchical communications on territories not equipped yet with RSU: in the case no RSU is detected by the car, the TCU (Telecommunication Control Unit) of the vehicle will send the data to a back-end server using the cellular network.

This hybrid solution may also exist in the long term. On particular territories such as secondary roads, one could consider an unbalance between benefits and investments in G5 technology. The socio-economic studies should highlight such a situation.

Benefits of a direct link for the driver:

* Direct (i.e. reliable) information from the road operator, even for unplanned interventions
* Direct information from other vehicles, automatically triggered (i.e. reliable, with no interpretation)
* An optimized HMI
* No intermediate involving optimized costs according to free-to-free principle

Benefits of this direct link for the road operator

* Access to speed data, directly aggregated in Datex, without loops or buying FCD
* Access to reliable event data
* No intermediate: no additional costs
* Provision of direct information to drivers, at any place (no need for a VMS)
* Possibility to send accurate information on (even unplanned) road works (road workers‘ safety)
* Possibility to send information directly from road operators‘ vehicles intervening

SCOOP privacy and security solution

* Connected vehicles are going to create new technological and economic challenges in the automotive industry. Communication use for will have to be secured and anonymized. Interoperable cooperative vehicles will be based on a system of safety management for communications and prepare a reliable and secure systems for future connected autonomous vehicles at the end.
* These communication systems require security and digital trust, where vehicles and roadside equipment have to use digital certificates in order to secure data exchanges and trust ITS identities. This means implementing a security management infrastructure based on Public Key Infrastructure (PKI) concepts.
* Trust and privacy management requires secure establishment and maintenance of trust relationships for communication.

This may be enabled using security parameters such as identity or properties which are guaranteed by trusted third parties (Certification Authority): certificates for proof of identity named Enrolment Credentials or others such as Authorization Tickets (AT). Public key certificates and Public Key Infrastructure (PKI) are used to establish and maintain trust between the ITS-S and between ITS-S and authorities.