



Rijkswaterstaat
Ministry of Infrastructure
and Water Management

Cooperative ITS Corridor Validating the interoperability of PKI solutions

Rijkswaterstaat's Cooperative ITS Corridor project is now focussing its efforts on following up previous developments and testing. Based on the results of the previous phases, the project is further addressing open issues and looking at new ones. Among other things, specific steps are being taken to solve the complex subject of internationally interoperable security.

The Cooperative ITS Corridor project has tested the requisite Public Key Infrastructure (PKI) for cooperative driving on the Dutch Corridor section of the A16 motorway near Dordrecht. In order to validate the international interoperability of the system, Rijkswaterstaat participated in the InterCor PKI Security TestFest in April 2018.

This interoperability event was organised by the – partly EU-financed – InterCor project and specifically by InterCor partner University Reims Champagne-Ardenne in France. The InterCor (Interoperable Corridors) project aims to enable vehicles and road infrastructure to communicate data through cellular or ITS-G5 networks, or a combination of both, on road corridors through the four member states of France, Belgium, the United Kingdom and the Netherlands. In this project technical specifications are validated in a broad context in order to enable the roll-out of interoperable C-ITS services. The Dutch part of the Cooperative ITS Corridor project is the technical core of the Dutch contribution to InterCor.

Objective of the PKI Security TestFest

The objective of the PKI Security TestFest was to validate the international interoperability of cooperative PKI solutions, including the authentication of messages exchanged between ITS stations from different regions.

Cross-border intelligent mobility

The C-ITS Corridor project is a cooperation of road operators in the Netherlands, Germany and Austria. Together with industrial partners, the road operators are working towards the introduction of cooperative services in Europe.

Initially, the Cooperative ITS Corridor focussed on two services:

- Road Works Warning (RWW)
- Probe Vehicle Data (PVD, sensor data from vehicles)

The Netherlands is additionally also developing:

- Collision Risk Warning (CRW, stationary vehicles warning)
- In Vehicle Signage (IVS)

The Cooperative ITS Corridor project has carried out large-scale tests (pre-deployments) on various stretches of the Dutch section of the Corridor Rotterdam–Frankfurt–Vienna, it has also participated in similar tests ('Probetrieb') in Hessen (Germany) and has organised the first TestFest of the InterCor project. These tests provided the project team with a solid basis for the technical specifications of the services. These results were shared with the C-Roads platform to contribute to complete harmonisation at European level.



Test approach

Participants from 11 countries tested different security scenarios on a 23 kilometre loop along the motorway near Reims, with the services RWW using DENM messages and PVD using CAM messages. Validation was done by testing the interoperability of systems, both on-board (OBUs) as well as at the roadside (RSUs). The focus was on service interoperability rather than on product interoperability. A number of OBUs from various suppliers from different countries, with different certificate authorities, were tested against a number of RSUs with identical as well as different certificate authorities.

Using a dedicated test vehicle, equipped with a specific 'validation OBU', Rijkswaterstaat tested various security scenarios based on these services. To further enable interoperability and cross-border testing, Rijkswaterstaat also installed a Dutch portable RSU at the test site.

The main security-PKI functionalities tested were:

- Message signature/verification
- The use of pseudonym certificates
- Trust chain verification

Main results and lessons learned

The C-ITS Corridor project obtained valuable results and learned valuable lessons from the PKI Security TestFest. We learned that, from a technical point of view, the PKI solutions function as required and that it is technically possible to realise internationally interoperable PKI solutions. However, the results also showed that fundamental choices have to be made on variables, which are

left open by the standards. And again it became clear that interoperability cannot be achieved without agreements on these variables ('profiling'). Last but not least, the C-ITS Corridor project obtained significant insight into the organisational infrastructure required to support internationally interoperable PKI solutions.

Reporting

A report of the PKI Security TestFest has been published on the [InterCor website](#).

Participants in the project

- Compass
- Dutch Department of Motor Vehicles (Dienst Wegverkeer, RDW)
- Swarco
- UL
- V-Tron



Published by **Rijkswaterstaat**
For further information visit www.intercor-project.eu
or www.its-corridor.nl
November 2018 / PPO1118TP355