Deliverable: Solution paths to enhance C-ITS interoperability in Europe

Activity 4 Cross-Test

Sub Activity: 4.3

Version 1.0

Publication Date: 31/12/2019

Co-financed by the Connecting Europe Facility of the European Union

Information on the document

Document: Solution paths to enhance C-ITS interoperability in Europe

Date of publication: 31/12/19

Responsible, Entity: Hasnaâ ANISS, IFSTTAR

Status: Version 1.0

Publication

Date	Version	Author(s)	Updates & changes	Diffusion
31/12/2019	1.0	Cross-test team	Final document	Public

Reference to the version administration

Version number to be composed of 3 digits > vR.XY
- R corresponds to the release number: it is upgraded each time SC Studies validates the diffusion of a new release,
- X is the major version number: it is upgraded each time SC Studies validates the deliverable,
- Y is the minor version number: it is upgraded each time a contributor changes anything.

Once the deliverable is approved, its version number is upgraded from vR.XY to vR.(X+1)0
Once the deliverable is release, its version number is upgraded from vR.XY to v(R+1).00

As illustration:
0.03 > Work in progress version
0.10 > Del. Approved by SC Studies but not released
2.00 > Del. approved & released (in release 2)
2.05 > Del. Updated - in progress version

Table of Contents

Table of Contents 3
1 Introduction 4
2 Recommendation for security aspect 4
2.1 Governance and PKI 4
2.2 Interoperability and backward compatibility between different security standards 5
3 Recommendation for hybrid communications - Roaming from one cellular network to another 6
4 The need for profiling of standards to ensure interoperability at application level 7
5 ASN1 issues 7

1 Introduction

During SCOOP@F project, several studies were conducted in order to assess the interoperability between countries.
Spain, Portugal, France and Austria dedicated resources to analyze each specification, determine interoperability risks and organize cross test session in laboratory, in test tracks and in open road.

Two test series were conducted: one with a focus on ITS-G5 communications with selected use cases, the second on hybrid communications, both with and without security.

During these tests:

- Spanish vehicles went in France, Portugal and Austria
- Portuguese vehicles went in France, Spain and Austria
- French vehicles went in Spain, Portugal and Austria.

Therefore, vehicles from 3 countries were able to communicate with security with R-ITS-S and National central ITS-S belonging to the participating four countries. The four years experiences on interoperability allow us to draw the following lessons and propose ways to improve European cross-border interoperability.

2 Recommendation for security aspect

2.1 Governance and PKI

Cross-tests allowed the identification of the following topics that needs to be considered for European wide C-ITS deployment:

- Governance of an interoperable and a global Public-Key Infrastructure for a European wide C-ITS security Credential Management system
- In order to ensure interoperability among the different PKIs deployed by the European countries, a specific care has to be considered regarding the C-ITS Security Credential Management System.
- A secured C-ITS system is built on top of the notion of trust, which is materialized in the PKI by a Trust List Manager. This Trust List Manager needs to be updated with the required certificates so that the different PKIs can be integrated into the same trust domain.

To achieve this goal a common EU-wide cybersecurity infrastructures and processes are needed for secure and trustful communication between vehicles and road infrastructures to provide C-ITS road safety and traffic management services.

The cross-tests highlighted the importance and the necessity of having a governance policy for the management of the trust lists between different countries. When the Trust lists are not updated with the required certificates, C-ITS messages coming from foreign countries are rejected by the V-ITS and R-ITS Stations because the senders are considered not part of the trust domain. As a consequence, the envisioned C-ITS services cannot be provisioned.

Before the full operation of a “Production” ECTL for at-scale deployments, we identify the needs for intermediate “pre-production” ECTLs aimed at testing cross border interoperability.

2.2 Interoperability and backward compatibility between different security standards

Currently, two concurrent ETSI security standard versions exists the TS 103 097 v1.2.1 and the TS 103 097 v1.3.1. These two versions are not backward/forward compatible.
The TS 103 097 is an important standard which specifies in detail the secure data structure and the header certificate formats to be implemented by each C-ITS station enrolled in the trust domain.

These second series of cross-tests highlighted the importance of deploying the same security standard in order to ensure full interoperability between the different countries. To manage the coexistence of 2 different versions of security standards, an additional component has been introduced, taking in charge the mapping of the security header field of a C-ITS message from one standard version to another standard.

This solution works only for long-range communications between different countries but not for short-range communication. The consequence of this latter solution is the loss of end-to-end authentication between the originating C-ITS station and the receiving C-ITS station.

We recommend to have a specific monitoring of standard evolution to foster security improvements with continuous retro compatibility.

3 Recommendation for hybrid communications - Roaming from one cellular network to another

Each V-ITS-S equipped with cellular communication technology is associated to its home cellular network. When a vehicle travels outside the coverage area of the home network, the V-ITS-S uses the visited cellular network when it is available and when V-ITS-S cellular subscription enables roaming.

The roaming process involves the usage of the location update procedure that determines the location of the mobile station by identifying the geographical coverage area of a base station, it is connected to.

When the mobile station is turned on in the visited network, the latter notices that it is not registered with its own system and attempts to identify its home network. If there is no roaming agreement between the two networks, maintaining the cellular is impossible, and consequently the visited network denies the service.

When there is a roaming agreement between the two networks, the visited network contacts the home network and requests service information including whether the mobile should be allowed to roam. If the request is successful, the visited network maintains a temporary subscriber record for the device. Likewise, the home network updates its information to indicate that the mobile station is on the visited network so that any information sent to that device can be correctly routed.

When the roaming is successful, the visited network provides a new IP address to the mobile station. The new IP address attribution results into the interruption of the communication session between the V-ITS-S and the National node. Then, the V-ITS-S must establish a new communication session with the National Node.

The roaming process induces communication delays and interruptions during the handover between the home network and the visited network.

This second series of cross-tests has shown in real conditions the 2 types of roaming situations, respectively "V-ITS-S with no roaming agreement" and "V-ITS-S with a roaming agreement".

These aspects have also to be considered for an EU-Wide deployment of C-ITS by finding solutions which allow a seamless connection during the roaming, by having information redundancy at the border or by prioritizing ITS-G5 at the border.

4 The need for profiling of standards to ensure interoperability at application level

Though many C-ITS related standards already developed are largely adopted (when not mandated) by existing C-ITS deployments (as it was the case for the sites participating in the SCOOP XTest activity), practical implementations may still encounter interoperability issues at application level due to the different usage of these standards in terms of both the use/not use of optional fields and even the values adopted for these fields and even for the mandatory ones.

As achievement of long-term societal benefits at EU level by an effective deployment of C-ITS systems is clearly dependent of the full interoperability of these systems, a common profiling taking into account implementation needs should be dealt and maintained.

5 ASN1 issues

It is vital for interoperability that all stakeholders use EXACTLY the same ASN structure to encode and decode C-ITS messages. Indeed, when information are exchanged in PER, the "naming" information of the data elements or data fields are removed from files to ensure that data exchange is as light as possible. The technical counterpart is that sender and receiver shall use the same known structure(s) or the device won't speak the same language and won't be able to understand them each other.

Examples:

1 / We know that the new CDD (1.3.1) has changed the order of the lanes in its text (numbering from inside the road now). However, the ASN code contained in the document CDD (1.3.1) says that it is numbered as before (numbering from outside the road). Some C-Roads partners have explained that ongoing developments had been done with the logic of numbering the lanes contained in the text part (from inside to outside). They probably therefore use neither exactly the ASN of the new CDD (1.3.1), nor the ASN of the previous CDD (1.2.1).

Then, what ASN coding (exact structure) has been used? Is it the one contained in CDD 1.3.1 with an unofficial correction on the sense regarding lane numbering, to fit with the textual part?

2 / The (ex) DA annex II quotes 103 301 V1.2.1 and 19 091 V2017-03
103 301 1.2.1 contains a SPATEM / MAPEM ASN which calls 19091 profile 2 dsrc 2 version 2. That is to say the ASN which is there: https://standards.iso.org/iso/ts/19091/ed -2 / in and which is that of edition 2 of 2019-06 (and not 2017-03).
By consequence, it is obviously not the ASN which is there:
https://standards.iso.org/iso/ts/19091/addgrp_c and which is that of edition 1 of 19 091 (i.e. the document of 2017-03).
Thus, there is a discrepancy that partners shall overcome to ensure interoperability without any doubt (by using the same ASN).

3 / The (ex) DA annex II quotes 103 301 1.2.1 and 19 321 2015-04.
103 301 1.2.1 contains an IVIM ASN which calls 19321 version 1. So far, no problem. However, some European partners seemed to be eyeing 19321 in progress, whose ASN is already available here: https://standards.iso.org/iso/ts/19321/ed-2.
There is no discrepancy but partners have to ensure they will use the same ASN structure.
All those examples are here to say that we collectively (at European level) shall be very clear about the ASN that we use, otherwise it will be problematic at the level of interoperability.