Use case scenarios with security data

Delivrable 2.4.4.6.bis

Activity 2.4.4

Version 1.0

Publication Date : March 16, 2015

Information on the document

- Transmitter (Organization) : Télécom ParisTech

- Editor: Houda LABIOD, Ahmed SERHROUCHNI, Pascal URIEN, Ali ATOUI

- Statuts (in progress, finalized, approuved) : finalized

Publication history

Date	Version	Redactors	Principal modifications	Dissemination
March 16, 2015	1.0	Houda LABIOD Ahmed SERHROUCHNI Pascal URIEN Ali ATOUI		SCOOP@F

Table of Contents

Table of figures

Table of tables

Abbreviations

CAM	Cooperative Awareness Message
CIGT	Centre d’Ingénierie et de Gestion de Trafic
DENM	Decentralized Environmental Notification Message
ITS	Intelligent Transport System
OD	Operator Devices
PC	Pseudonym Certificate
RSU	Roadside unit
SAGT	System d’Aide a la Gestion du Trafic
TG	Terminal du Gestionnaire
TMEC	Traffic Management and Engineering Center
TMSS	Traffic Management Support Systems
V2I	Vehicle to Infrastructure Communication
V2V	Vehicle to Vehicle Communication

1- Objective

The main goal of this document is to describe the way that a use case is executed. Since we have two types of messages (CAM and DENM) and different communication modes (V2V, V2I and I2V), we are going to present two different use cases in order to cover the whole process.

2- Use case A1: uploading circulation data (Données de Circulation)

This use case consists on automatically collecting and uploading circulation data such as the position, heading, speed, etc. The message uploaded is a CAM message that contains all necessary data. The source of the message is the ITSS-V and the destination is the TMEC (Traffic Management and Engineering Center (CIGT)), including the platform (ITSS-C) and the TMSS (Traffic Management Support System (SAGT)). The figure below shows the scenario of the use case.

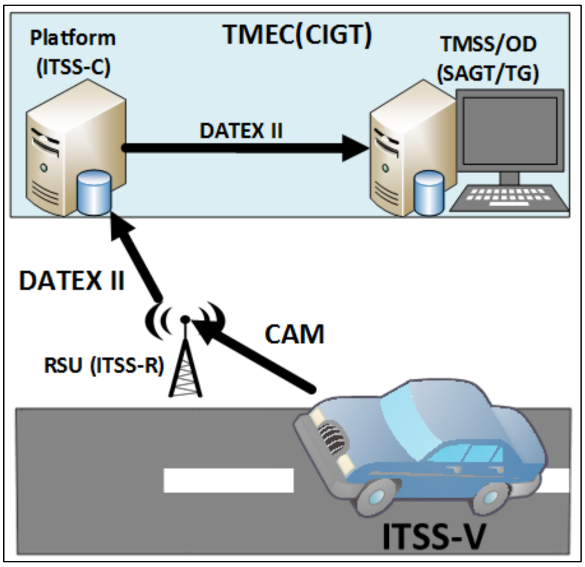


Figure 1: Uploading circulation data.

The ITSS-V generates and broadcast a CAM message. The message is received by the ITSS-R, translated to DATEX II format and forwarded to the TMEC. Figure 2 shows more details about this use case.

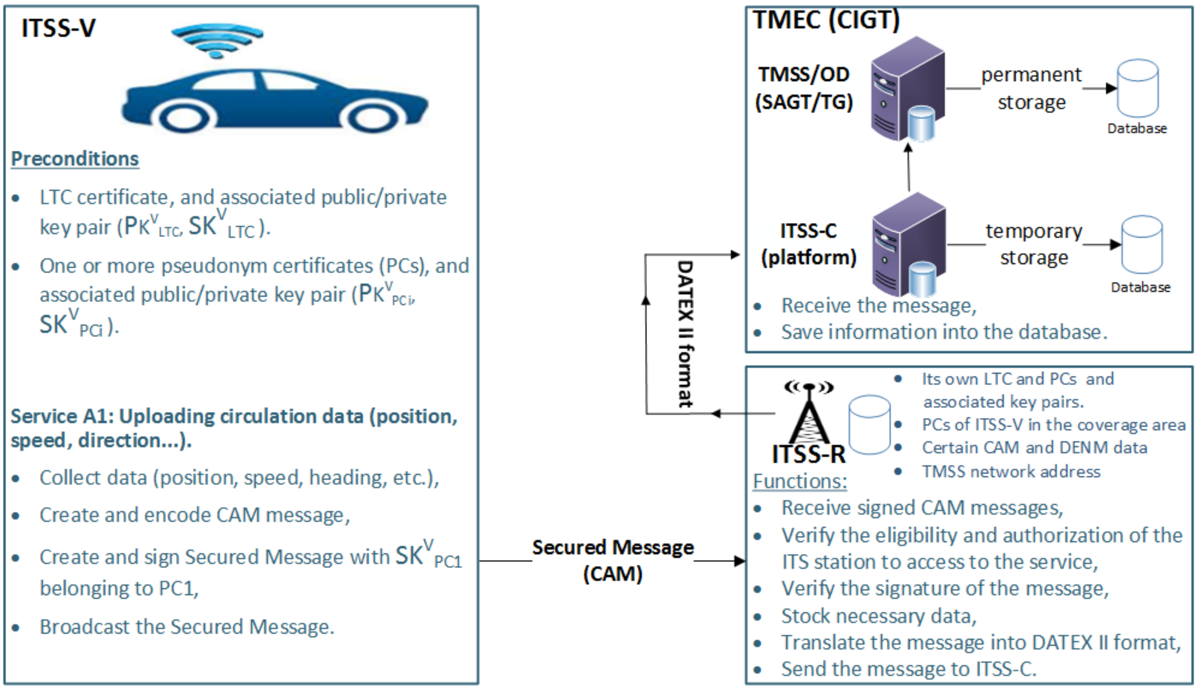

ITSS-V
Preconditions
LTC certificate, and associated public/private key pair (PK^{V}_{LTC}, SK^{V}_{LTC}).
One or more pseudonym certificates (PCs), and associated public/private key pair (PK^{V}_{PCi}, SK^{V}_{PCi}).
Service A1: Uploading circulation data (position, speed, direction...).
Collect data (position, speed, heading, etc.),
Create and encode CAM message,
Create and sign Secured Message with SK^{V}_{PC1} belonging to PC1,
Broadcast the Secured Message.
Secured Message (CAM)
DATEX II format
TMEC (CIGT)
TMSS/OD (SAGT/TG)
permanent storage
Database
ITSS-C (platform)
temporary storage
Database
Receive the message,
Save information into the database.
Its own LTC and PCs and associated key pairs.
PCs of ITSS-V in the coverage area
Certain CAM and DENM data
TMSS network address
ITSS-R
Functions:
Receive signed CAM messages,
Verify the eligibility and authorization of the ITS station to access to the service,
Verify the signature of the message,
Stock necessary data,
Translate the message into DATEX II format,
Send the message to ITSS-C.

Figure 2: Scenario of the use case A1.

To send the signed CAM, ITSS-V uses a valid pseudonym certificate. The scenario of the use case A1 is described as follows:

ITSS-V

1- Generates the CAM message, which contains information about the station and the traffic,
2- Builds the secured message (see figure 3),
3- Signs the secured message using the private key SK^{V}_{PC1} associated with the pseudonym certificate PC1, and
4- Broadcasts the secured message.

ITSS-R

1- Receives the secured message
2- Checks the header field, and particularly the signer info,
   a. <u>Case 1:</u> the signer_info is a **certificate_digest_with_sha256** of the PC1 belonging to the ITSS-V. The ITSS-R has already received the entire certificate PC1.
   The ITSS-R verifies the digest, it calculates the hash of the certificate PC1 using sha256, compares the result with the value contained in the secured message, if the hashes are similar, the ITSS-R can trust the sender and processes the secured message.
   b. <u>Case 2:</u> the signer_info is a **certificate_digest_with _sha256** of the PC1 belonging to the ITSS-V. The ITSS-R does not have the corresponding entire certificate (PC1).

In such case, the ITSS-R sends a CAM message with header field of type request_unrecognized_certificate, requesting the ITSS-V its entire PC1.

c. Case 3: The signer_info is a certificate or certificate_chain. The ITSS-R verifies the certificate's validity and legitimacy, and saves it in its database. Verifying the certificate consists of verifying the validity date and the signer_info of the certificate. The signer_infor should be the certificate or the certificate digest of the CA that issued the ITSS-V's certificate.

3- The ITSS-R verifies the authorization of the ITSS-V to send CAMs messages, by verifying the its-aid included in the Secured Message and whether it matches with the SSP list included in the certificate.
   a. Case 1: The its_aid that exists in the Secured Message do not match with the SSP list existing ITSS-V's certificate. The ITSS-V is not allowed to access this type of service (sending CAM), and the message is rejected.
   b. Case 2: The its_aid matches with the SSP list and the message is accepted.

4- Once the eligibility and authorization of the ITSS-V are verified, the ITSS-R verifies the signature of the messageIt deciphers the signature value with the public key associated with the PC1, obtains the hash result, calculates the hash of the message, and finally compares the two hashes.
   a. Case 1: The two hashes are not similar. The signature is not valid, the message is rejected.
   b. Case 2: The two hashes are similar. The signature is valid and the message is accepted.

5- If the signature is valid, the ITSS-R puts the CAM's payload into DATEX II message format.

6- The ITSS-R sends the new message to the TMEC (ITSS-C and TMSS) through a secure Ethernet communication.

ITSS-C

1- Receives the DATEX II message and stores permanently some specific information.

TMSS/OD (SAGT/TG)

1- Receives the DATEX II message,
2- Stores some specific data,
3- Analyzes information and takes decisions.

The figure 3 shows the structure of the secured message for CAM [2].

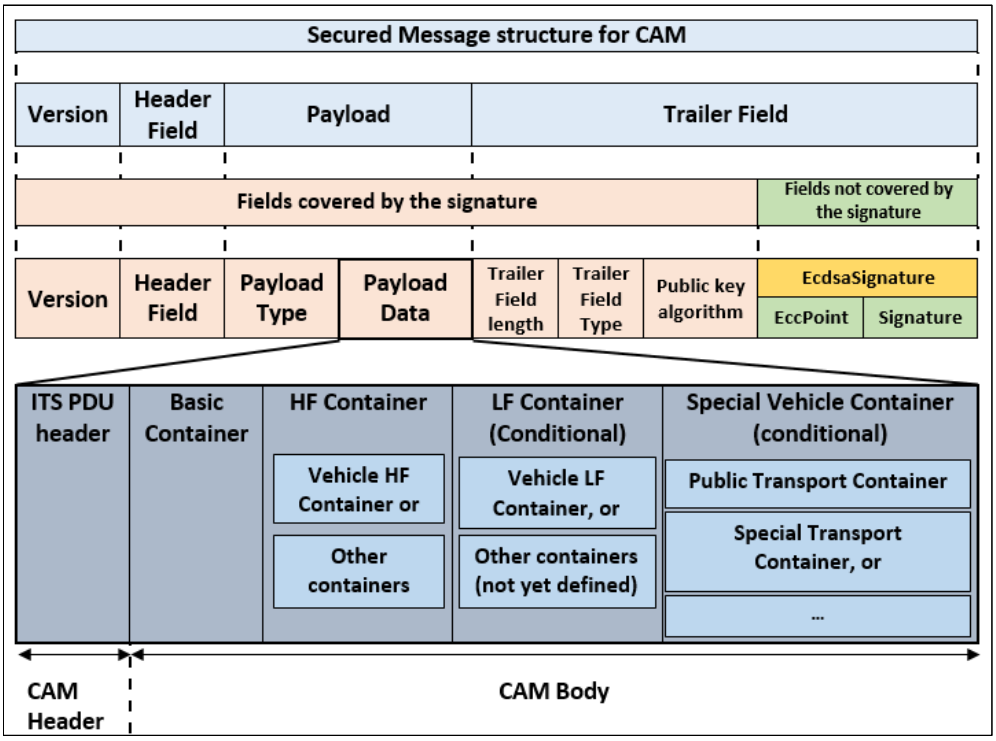


Figure 3: The structure of a Secured Message for CAM.

In the following we present a general description of the secured message's contents:

1- The version filed contains the protocol version of the secured message, the current protocol version is 2.
2- The Header field contains the:
    a. Signer_info which is a certificate or a certificate digest that identifies the signer (issuer) of the message. The signer_info type can be :
        i. Certificate_digest_with_sha256: An 8 octet digest of the certificate belonging to ITSS-V.
        ii. Certificate: The certificate of the ITSS-V (in this case it is the PC1).
        iii. Certificate chain: The complete certificate chain up to the Root CA or a subordinate CA.
    b. Generation time of the message.
    c. Its_aid which indicates the type of the service (sending CAM, sending DENM).
    d. Request_unrecognized_certificate: it shall be included if an ITS-S received CAMs from other ITS-Ss, which the ITS-S has never encountered before and which included only a signer_info field of type certificate_digest_with_sha256 instead of a signer_info of type certificate. In this case the signature of the received CAMs cannot be verified because the verification key is missing.
3- Payload which contains the CAM payload.
4- Trailer field, it contains the public key algorithm used to sign the message and the signature itself.

The data that should be uploaded in any CAM message is presented in the table 1.

Data that should be uploaded in CAMs	Description
Station Type	0= unknown, 4=motorcycle, 5=passenger Car, 6=bus, 15= roadside Unit …
Reference Position	The geographical position of a location or of an ITS station: latitude, longitude, position Confidence Ellipse, altitude.
Heading	Heading direction with regards to the WGS84 north and the accuracy of the heading value.
Speed	It describes the speed and corresponding accuracy of the speed information for a moving object (e.g. vehicle).
Drive Direction	It denotes whether a vehicle is driving forward or backward.
Vehicle Length	Estimated length of vehicle and whether the estimated length is confident.
Vehicle Width	Estimated width of vehicle, including side mirrors.
Longitudinal Acceleration	It indicates the vehicle acceleration at longitudinal direction and the accuracy of the longitudinal acceleration.
Curvature	It describes the curvature of the vehicle trajectory and the accuracy of the provided curvature. The curvature detected by a vehicle represents the curvature of actual vehicle trajectory.
Curvature Calculation Mode	It describes whether the yaw rate is used by vehicle to calculate the curvature as provided by the Curvature data type.
Yaw Rate	Yaw rate of vehicle at a point in time.
Vehicle Role	0=default, 1= public Transport, 2=special Transport, 3= dangerous Goods, 4= road Work, 5=rescue, 6=emergency, 7=safety Car ….
Exterior Lights	0=Exterior Lights low Beam Head lights On, 1=high Beam Head lights On , 2=left Turn Signal On , 7=parking Lights On …
Path History	DF that defines a path with a set of path points. It may contain up to 23 Path Points. It may be used to describe the historical path of a vehicle or any path.
Special Transport Type	0=Heavy Load,1=Excess Width, 2=Excess Length, 3=Excess Height …
Dangerous Goods Basic	0=Dangerous Goods Basic explosives1, 6=flammable Gases, 8=toxic Gases…
Protected Communication Zones RSU	Information about position of a CEN DSRC Tolling Station operating in the 5.8 GHz frequency band. If this information is provided by RSUs a receiving vehicle ITS-S is prepared to adopt mitigation techniques when being in the vicinity of CEN DSRC tolling stations.
Generation Delta Time	Time of the CAM generation

Table 1: Data that should be uploaded in a CAM message [1].

3- Use case A3 & D2: Uploading event data declared by the driver & Animal on the road warning

In this example, we describe how an information uploaded can be used to provide another service. The use case A3 consists on manually declaring events on the road. The driver can use an HMI for declaring the presence of an animal on the road. At the moment where the driver touches the HMI, the geographical position is retrieved and a request is sent to the appropriate application. The application generates a DENM message and the ITSS-V broadcast it. The process of capturing the message by the ITSS-R, translating it to DATEX II format and sending it to the TMEC (CIGT) is similar to the process described for use case A1 (see section 2). The message content is different, since it is a DENM message. Other vehicles in the same area, also can receive the DENM message and be notified. The table below shows the content of a DENM message.

Name of the container	Data element (DE)	Description
Management Container	Action ID	Identifier generated by the DEN basic service for new DENM.
	Detection Time	Time at which the event is detected by the originating ITS-S.
	Reference Time	This DE refers to the time at which a new DENM, an update DENM or a cancellation DENM is generated.
	Termination	This DE indicates if the type of generated DENM is a cancellation DENM or a negation DENM.
	Event Position	Geographical position of the detected event.
	Relevance Distance	The distance in which event information is relevant for the receiving ITS-S, starting from the event position.
	Relevance Traffic Direction	The traffic direction along which the event information is relevant for the receiving ITS-S.
	Validity Duration	Validity duration of a DENM set by the originating ITS-S.
	Transmission Interval	Time interval for DENM transmission as defined by the originating ITS-S.
	Station Type	This DE provides the station type information of the originating ITS-S.
Situation Container	Information Quality	Quality level of the information provided by the ITS-S application of the originating ITS-S. It indicates the probability of the detected event being truly existent at the event position.
	Event Type	Description for the event type, including direct cause and sub cause.
	Linked Cause	Description for a linked event of the provided *eventType*, including direct cause and sub cause of the linked event.
	Event History	The DF consists of a list of event points which represents the dimension of a plain event in a predefined order. In case that the plain event is detected by a vehicle ITS-S, the DF consists of a list of event detection points along the path that the detecting ITS-S has travelled over some past time and/or distance. Each event point corresponds to a point at which the same event was detected along the path.
Location Container	Event Speed	Moving speed of a detected event and the confidence of the moving speed information.
	Event Position Heading	The heading direction of the event and the confidence of the heading information, if applicable.
	Traces	This DF is the location referencing information of *eventPosition*. It includes a group of traces

	Road Type	The road type information at the event position.
Stationary Vehicle Container	Stationary Since	This DE provides the time duration of the stationary vehicle being stationary.
	Stationary Cause	This DE provides additional information to describe causes of the stationary vehicle event such as human problem.
	Carrying Dangerous Goods	DF included in the *stationaryVehicle* DF in the *alacarte* container if a vehicle carrying dangerous goods is involved in a stationary vehicle event. It provides information on the type of dangerous goods, the required emergency action and other information.
	Energy Storage Type	This DE provides the vehicle energy storage type information of the stationary vehicle as specified.
Alacarte Container	Lane Position	The lane position of the event position in the road counted from the outside boarder of the road.
	External Temperature	Information included in the *alacarte* container for the adverse weather condition use case.
	Positioning Solution	It indicates the positioning technology being used to estimate a geographical position.
Stationary Vehicle		It provides information of the stationary vehicle.
Default Validity		600ms
Termination		ENUMERATED {isCancellation (0), isNegation (1)}.

Table 2: Data that should be uploaded in a DENM message [1].

The TMEC (CIGT) receives several messages from different sources, declaring that an animal is on the road. After consolidation of the information, it generates a warning message and sends it to the ITSS-R to be broadcasted (or geo-broadcasted) to all vehicles in the target area. The target area should be 400 m before the event area, the frequency of the broadcasting is 1s to 4s during 180s to 300s depending whether the target area is an urban or rural area [1].

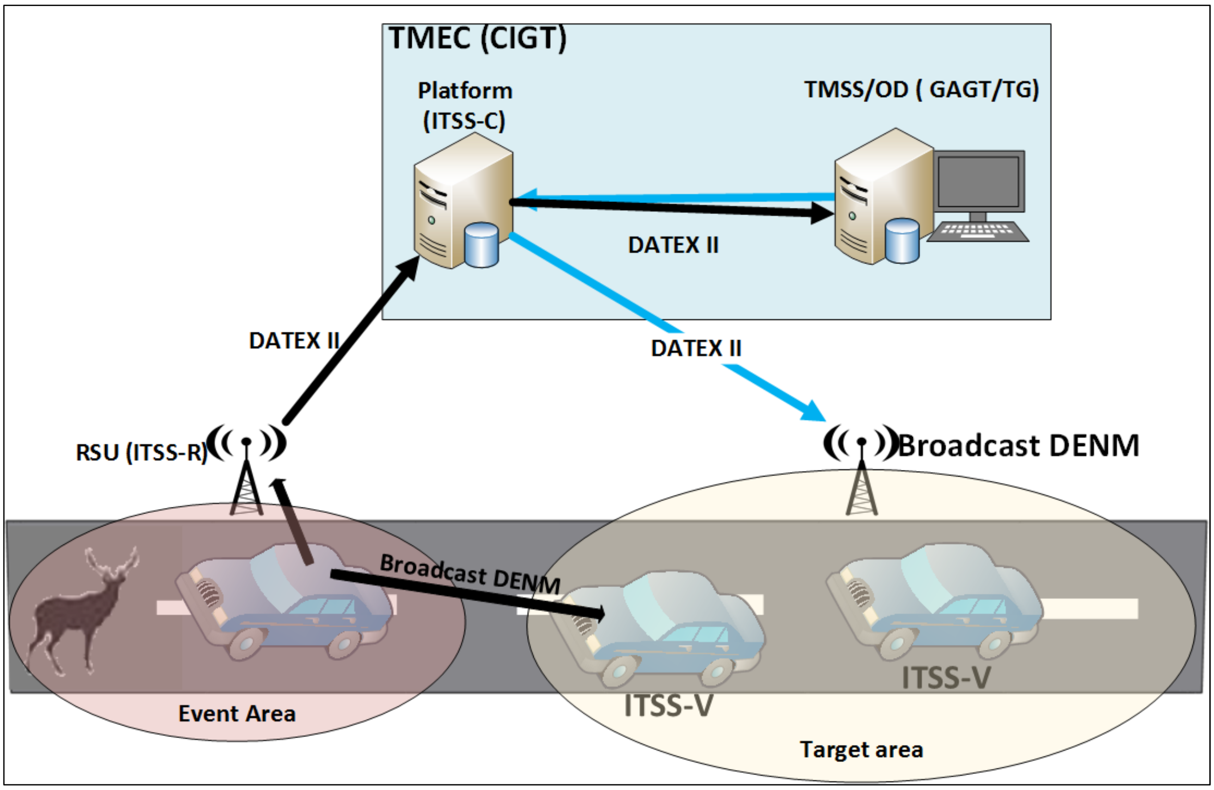


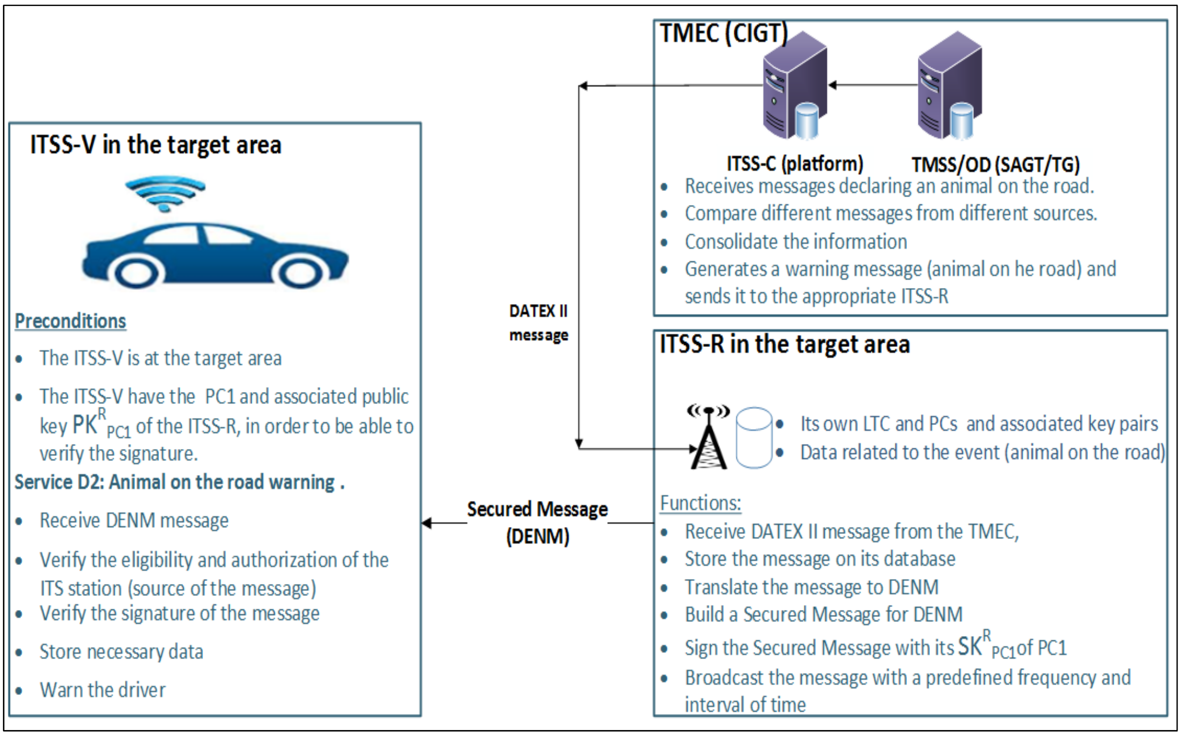
Figure 4: Animal on the road use case.

For the V2I and V2V communication, the DENM message broadcasted by the vehicles should be signed as explained in the use case A1, otherwise the message will be rejected by the receiving entities (ITSS-R and ITSS-V).

Whereas, for the I2V communication, the warning message generated by the TMSS (SAGT) should be signed by the ITSS-R before broadcasting it.

In the figure 5 the TMSS/OD (SAGT/TG) builds a warning message about an animal on the road, and sends it to the ITSS-R in a DATEX II format. The ITSS-R translates the message to DENM, builds and signs a secured message for DENM and finally broadcasts it to all ITSS-V in the coverage area.

All vehicles in the target area, receives the message and verify the signature. If the signature is valid, it means that it comes from an eligible source, the warning message will be transmitted to the driver through the HMI.



- Receives messages declaring an animal on the road.
- Compare different messages from different sources.
- Consolidate the information
- Generates a warning message (animal on he road) and sends it to the appropriate ITSS-R

Preconditions

- The ITSS-V is at the target area
- The ITSS-V have the PC1 and associated public key PK^{R}_{PC1} of the ITSS-R, in order to be able to verify the signature.

Service D2: Animal on the road warning .

- Receive DENM message
- Verify the eligibility and authorization of the ITS station (source of the message)
- Verify the signature of the message
- Store necessary data
- Warn the driver

- Its own LTC and PCs and associated key pairs
- Data related to the event (animal on the road)

Functions:

- Receive DATEX II message from the TMEC,
- Store the message on its database
- Translate the message to DENM
- Build a Secured Message for DENM
- Sign the Secured Message with its $SK^{R}_{PC1}$of PC1
- Broadcast the message with a predefined frequency and interval of time

Figure 5: Scenario of the use case D2.

4- Conclusion

In this deliverable two use cases are detailed in order to better understand the process of exchanging data through some SCOOP@F part 1 use cases. We choose two different use cases to cover all types of communication (V2V, V2I and I2V), and both CAM and DENM messages.

Bibliography

[1] Livrable 2.4.1 v0.2, Novembre 2014 - Spécifications de l'architecture fonctionnelle.

[2] ETSI TS 103 097 V1.1.15 (2014-11) Intelligent Transport Systems (ITS); Security; Security header and certificate formats.